Government of Alberta

Health and Wellness

Project Name: Alberta Netcare Portal (ANP) Privacy Impact Assessment (PIA)

Contact Information:			
PIA Contact	Business Area Contact	Responsible Affiliate	
Troy Shostak	Martin Tailleur	Wendy Robillard	
Privacy Manager	Sr. Manager	Sr. Manager	
Information Compliance and	Electronic Health Records Delivery	Information Compliance and	
Access Unit	Services	Access Unit	
21 st Floor	Office of the CIO	21 st Floor	
10025 Jasper Avenue	14 th Floor	10025 Jasper Avenue	
Edmonton AB T5J 1S6	10025 Jasper Avenue	Edmonton AB T5J 1S6	
	Edmonton AB T5J 1S6		
Tel 780-422-8642	Tel 780-415-1427	Tel 780-422-5340	
Fax 780-422-1960	Fax 780-415-2289	Fax 780-422-1960	
E-mail: troy.shostak@gov.ab.ca	E-mail: martin.tailleur@gov.ab.ca	E-mail: wendy.robillard@gov.ab.ca	

PIA Submission Date: 13/10/2010

Expected Project Implementation Date: Already Implemented.

OIPC File Reference for any previously accepted PIAs that are related to this PIA:

- File # H0222 Electronic Health Record (EHR) Release 1.0 PIA (Part A)
- File # H0840 Capital Health (CH) netCARE
- File # H1124 Alberta Netcare Electronic Health Record Portal 2006
- File # H3213 Pharmaceutical Information Network (PIN)
- File # H0565, H0051 Person Directory (PD)
- File # F5260 Enterprise Information Management (EIM)
- File # H1556 Calgary Health Region (CHR) pHIE
- File # H0272 CH Enterprise Master Person Index (EMPI)
- File # H1397 Provincial Client Registry (PCR)
- File # H0229 Alberta Provider Directory (ABPD)
- File # H0375, H0771, H1941 Chronic Disease Management (CDM) information System (CH and CHR)
- File # H2335 Immunization/Adverse Event (Imm/AARI)
- File # H0039 Morbidity And Ambulatory Care Abstract Reporting (MACAR)
- File # H0226 AHW and CH Joint Laboratory Test Results History (LTRH)
- File # H0321, H0322, H0323 AHW, CHR and Calgary Laboratory Services (CLS) Joint Laboratory Clinical Data Repository (LCDR)



Section A: Project Summary

Evolution of the Alberta Netcare Electronic Health Record (Alberta EHR) and Alberta Netcare Portal (ANP)

The evolution of the Alberta Netcare Electronic Health Record (Alberta EHR) started with the alberta we//net's Limited Production Rollout (LPR) of the Seniors Drug Profile (SDP) System in the spring of 1999 to two Edmonton hospitals. The SDP System allowed authorized hospital clerical staff, nurses, pharmacists and physicians caring for seniors (65 years and older) to access dispensed Alberta Blue Cross (ABC) Group 66 Plan medication information from a secure environment and to facilitate making informed decisions regarding and, therefore, improve the quality of the patient's health care. In the fall of 1999, the SDP was also deployed to hospital emergency rooms across Alberta. In 2000, the SDP was further deployed to physician offices within Alberta.

In December 2001 the Premier's Advisory Council on Health (PACH) reported on a number of recommendations for health reform. Specifically, the PACH report recommended investment in technology and the establishment of an Electronic Health Record (EHR). In 2003 Alberta Health and Wellness (AHW) implemented the provincial EHR called the EHR-Release 1.0, also known as Portal 2004 (refer to Office of the Information and Privacy Commissioner (OIPC) File # H0222).

In June 2004 AHW, in collaboration with the former nine Regional Health Authorities¹ (RHAs), Alberta Cancer Board (ACB) and Alberta Medical Association (AMA), reviewed Alberta's existing EHR strategies (i.e. EHR, Capital Health's (CH) netCARE, and the non-metro health regions' EHR) and agreed to support a single, effective, common inter-jurisdictional EHR initiative for all users in the province.

In March 2006, the Capital Health (CH) netCARE platform (refer to OIPC File # H0840) was copied and adopted to become the Alberta Netcare web-based clinical portal which was named Alberta Netcare EHR-Portal 2006, also known as Portal 2006 (refer to OIPC File # H1124). In January 2008, the Portal 2006 and CH-netCARE were completely merged² creating a single instance referred to as Alberta Netcare Portal (ANP).

The ANP has been developed by AHW in cooperation and partnership with Alberta Health Services (AHS) and is continually evolving as other components become available, such as patient and provider registries as well as the addition of Electronic Medical Record (EMR) systems and Clinical Information Systems (CIS).

Please note the ANP, which is a web-based portal application that enables the electronic viewing of health information, is but one critical component (the viewer) of the entire Alberta EHR, which is Alberta's entire integrated electronic health record

1

RHAs included - Chinook, Palliser, Calgary Health, David Thompson, East Central, Capital Health, Aspen, Peace Country and Northern Lights.

² Portal 2004 and CH netCARE have been de-commissioned.

information system. This PIA only pertains to the ANP itself, and refers to the Alberta EHR as necessary to describe the functionality of the ANP.

More information regarding ANP and the Alberta EHR can be found online at http://www.albertanetcare.ca/.

Alberta Netcare Portal (ANP)

The Alberta Netcare Portal (ANP) Privacy Impact Assessment (PIA) is the first Alberta EHR-related PIA to be submitted by AHW since the recent proclamation of amendments to Alberta's *Health Information Act* (HIA) which now formally defines and acknowledges the existence of the Alberta EHR.

The ANP is the exclusive entry point/viewer for the Alberta EHR. It is a web-based clinical portal that enables authorized custodians and their authorized affiliates (i.e. authorized ANP users) to view patients' prescribed health information (as defined in s.56.1(c) HIA and the EHR Regulation) sourced from the Alberta EHR. In accordance with section 4 of the EHR Regulation, prescribed health information within the Alberta EHR includes information from AHS clinical systems³ and community-site clinical systems (i.e. private labs, physician, or pharmacist offices), such as:

- Patient Demographics via Person Directory (PD) (refer to OIPC Files H0565 and H0051);
- Laboratory Test Results (refer to OIPC Files H0326, H0321, H0322, H0323);
- Diagnostic Imaging (DI) Text Reports;
- Other transcribed clinical reports including
 - Discharge Summaries
 - Patient Histories
 - Consultation Reports
 - Operative Reports
 - Emergency Department (ED) Reports;
- Immunizations(refer to OIPC File H2335);
- Inpatient and Outpatient Admission and Discharge Events (refer to OIPC File H0039: and
- Patient Medication Histories via Pharmaceutical Information Network (PIN) (refer to OIPC File # H3213).

ANP Privacy Safeguards

Only authorized custodians as defined in the HIA can access the Alberta EHR. The HIA EHR Regulation section 3 provides the requirements that must be met for a custodian to become an authorized custodian. Within each authorized custodian's

³ TREP – Transcribed Reports Repository (Edmonton), RREP – Rural Report Repository, CHRP – EHR Index, CHAP – Capital Repository (houses Edmonton zone immunizations, home care summaries and ADT events), CHRLRP – Calgary Laboratory Repository, CHRDRP – Calgary Diagnostic Imaging Text Report Repository, CHRTRP – Calgary Transcribed Report Repository and LREP – Laboratory Repository (Edmonton) which is owned by the Edmonton Zone Laboratory team and is used by Dynalife – their laboratory provider. Components of prescribed health information within the Alberta EHR are located within these AHS clinical systems.

organization, only those affiliates who meet eligibility requirements, as confirmed by the authorized custodian's Access Administrator (AA), can become authorized users of the Alberta EHR (and therefore can access prescribed health information via ANP). The amount and type of prescribed health information each authorized user can access is based on user role. This means that access permissions and other security credentials are in place to ensure users have enough information to do their jobs and that information is accessed on a "need-to-know" basis. (Refer to Alberta Netcare Portal Permission Matrix in Appendix 16.)

ANP only enables viewing of information within the Alberta EHR; however, please note that section 56.4 of the HIA does require authorized custodians to consider any expressed wishes of the individual in deciding how much prescribed health information to make accessible via the Alberta EHR in the first place. Albertans may request that their prescribed health information be masked through a process called Global Person-Level Masking (GPLM). (Refer to Appendix 19.) All accesses to health records within the Alberta EHR are logged and recorded. Alberta EHR users are subject to fines, as stipulated in s. 107 of the HIA, and sanctions from their licensing and/or professional organizations if they use prescribed health information inappropriately and/or fail to consider expressed wishes in making it accessible via Alberta EHR. An authorized custodian must also submit a PIA which assesses privacy controls and ensures that practices and procedures within its organization/business adhere to the HIA.

ANP Security Safeguards

ANP is a securely-delivered, web-based application that can be accessed remotely via the internet with two-factor authentication (fob) or from a secure zone⁴ with valid user credentials.

Security measures include:

- Authorized custodians from community facilities such as private providers (including long term care organizations), physician offices, and pharmacies must conduct a Provincial Organizational Readiness Assessment (p-ORA), as they are outside of the secure zone. This tool assesses authorized custodians' administrative, technical and physical security controls in order to mitigate risks of accidental or malicious access to prescribed health information.
- Authorized custodians that are within the secure zone have met pre-established AHW Minimum Connectivity Requirements (MCR) and are not subject to p-ORA requirements. AHS facilities are deemed to be within the secure zone. Some long term care organizations and physician offices are located within AHS facilities. If they connect to the AHS network, then they would be considered to be within the secure zone.

⁴ 'Secure Zone' or 'Trusted Zone' is when ANP is accessed via specific ANP private URL (HTTPS) while 'Remote Access' or 'Untrusted Zone' is when ANP is accessed via the public internet (HTTP) and requires additional 2-factor authentication.

- All authorized ANP users must utilize a 'User Name' and 'Password' to enable ANP access. The 'User Name' and 'Password' validate that the users are who they say they are (authentication).
- Authorized ANP users are restricted to access prescribed health information based on the user role and profession (authorization), as per the Alberta Netcare Portal Permission Matrix (refer to Appendix 16).
- Authorized ANP users outside the secure zone, must use two-factor authentication to access ANP.
- Authorized ANP users within the secure zone do not require two-factor authentication to access ANP.
- All user-initiated activity is logged.
- AHW performs audits of information logs monthly, randomly, and on the request of patients or health services providers.
- All Alberta EHR users must be aware of the Terms of Use and Disclaimer for the ANP.

Benefits to Albertans

For patients, the Alberta EHR in general and the ANP in particular help improve the quality and safety of patient care by:

- Providing more accurate and up-to-date medical information about a patient;
- Presenting this information immediately at the point of care, which reduces delays in treatment, helps to ensure that the most appropriate treatment decisions are made, and improves health outcomes;
- Reducing the possibility of medical error by improving completeness, accuracy and clarity of medical records assessed at the point of care;
- Streamlining the secure sharing of prescribed health information between health service providers;
- Giving authorized health service providers a common understanding of a patient's medical condition, preventing the duplication of tests, unnecessary treatments and adverse events, such as harmful prescription drug interactions; and
- Reducing unnecessary duplication of tests, such as blood work.

For authorized custodians and their authorized affiliates (i.e. authorized ANP users), the Alberta EHR and ANP provide access to up-to-date information at the point of care by:

- Giving providers access to comprehensive key patient information along with online decision support and reference tools;
- Helping to reduce the possibility of medical errors, assist with compliance issues, and decrease the potential for adverse drug reactions;
- Helping to avoid the need to order duplicate tests by making previous data available; and
- Including features like lab value trends and drug monographs which can help with patient consultations.

Section B: Organizational Privacy Management

1. Management Structure

AHW Management Structure:

The Senior Manager of the Information, Compliance and Access Unit (ICAU) in the Health System Performance and Information Management (HSPIM) division has been delegated with the overall responsibility for privacy within the department. The AHW Privacy Manager, who reports directly to this Senior Manager, is subsequently tasked to manage privacy issues relating to AHW operations and will eventually oversee the implementation, application and monitoring of the Privacy Framework and Lifecycle for AHW. This will occur with the assistance of the AHW Privacy Advisors and in collaboration with the Policy and Security teams within ICAU. IM Policy 002 – 'Delegation of Oversight' establishes roles and the delegation of responsibility for the department under HIA (Appendix 1 – AHW Information Management Policies).

AHW has commenced the process of developing and will eventually pilot and implement a 'privacy framework', which will be an overarching mechanism to assist in setting direction with respect to privacy matters. It is intended to ensure a balance between the privacy rights of individuals with respect to their health and/or personal information and the legitimate needs of AHW in fulfilling its mandate. The 'privacy framework' is being designed to be a permanent, yet continually developing mechanism of direction and action that ensures that privacy risks for the Ministry are minimized and that AHW is compliant with privacy legislation.

The 'privacy framework' will be a model that encapsulates privacy principle's best practices and ensures that privacy risks are minimized and legislative requirements are met. It will also achieve the following objectives:

- Assist AHW in assessing its current level of privacy compliance;
- Identify any privacy gaps and potential risks to the Ministry;
- Propose mitigation strategies for identifiable privacy gaps or risks; and
- Establish mechanisms for continuous privacy compliance monitoring.

While this document does outline AHW privacy goals, a commitment to information privacy can also be found in most strategic corporate documents, illustrating a strong corporate commitment to health information privacy. AHW's Privacy Vision statement is as follows:

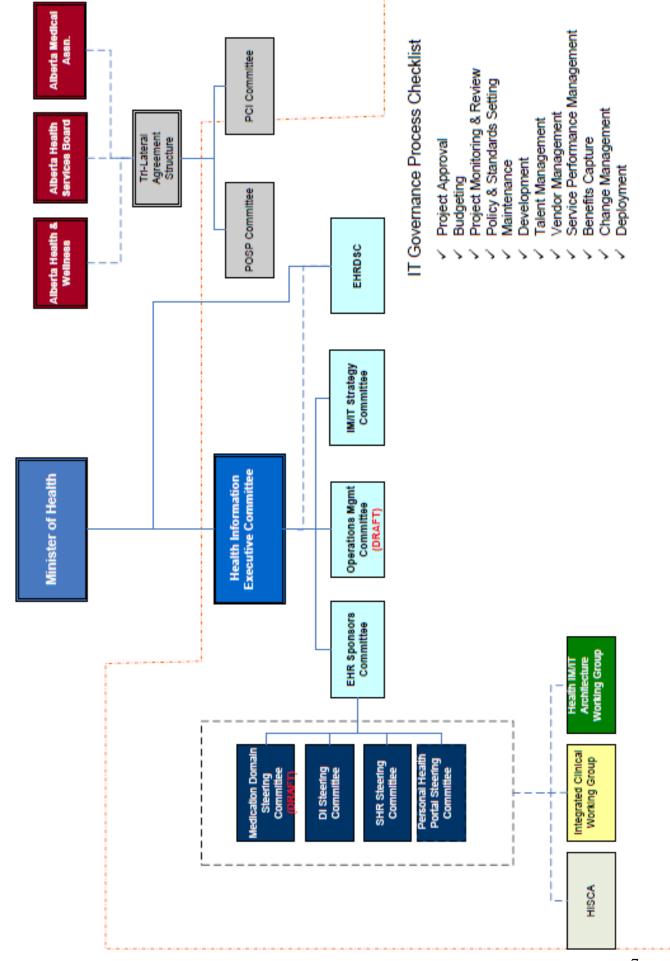
"AHW is a leader in health information privacy and complies with privacy principles and privacy legislation, and in doing so, further develop a standard of excellence which demonstrates integrity, transparency and accountability. By promoting privacy best

practices, we ensure that health and/or personal information is collected, used, disclosed, stored and disposed of only as required to carry out the legitimate needs of AHW in fulfilling its mandate and in accordance with privacy legislation."

Project Specific Governance Structure:

A copy of the current Provincial IM/IT Governance Structure is shown on page 7.

Provincial IM/IT Governance Structure



Since the inception of the Alberta EHR, AHW, as information manager of the Alberta EHR, has entered into an information manager agreement (IMA) with every custodian authorized to access information via the Alberta EHR. Section 2 of the new HIA EHR Regulation now formally designates AHW as information manager of the Alberta EHR.

The Health Information Executive Committee (HIEC) (Appendix 2 – Terms of Reference (TOR)) has authoritative responsibility to provide strategic leadership relating to intergovernmental initiatives surrounding the EHR and related e-Health initiatives. They report directly to the Minister of Health.

HIEC provides strategic leadership and support for the Alberta EHR and initiatives related to the publicly funded IM/IT health sector. The Provincial Information Sharing Framework (ISF) is a joint initiative between the AMA, CPSA, AHS and AHW to develop rules for how health information is generated from and shared with a physician's shared Electronic Medical Record (sEMR) or EMR may be collected, used and disclosed.

As per HIA section 56.7(1), AHW has established a stakeholder committee, with public representation, whose function is to make recommendations to the Minister with respect to the rules related to access, use, disclosure and retention of prescribed health information through the Alberta EHR. This committee is called the Provincial Electronic Health Record Data Stewardship Committee (EHRDSC). The EHRDSC is not a custodian, but develops rules on behalf of the collective of custodians.

The specific rules for using prescribed health information via the Alberta EHR are governed by the Alberta Netcare Information Exchange Protocol (IEP) (OIPC File #H1124). The IEP is incorporated by reference into the Alberta EHR IMA. All Alberta EHR users must adhere to the IEP. The rules in the IEP work in conjunction with the HIA and authorized custodians must ensure all authorized Alberta EHR users fully comply with the HIA and IEP when using prescribed health information via the Alberta EHR. Currently, the IEP is being revised to ensure consistency with the recent legislative changes to the HIA and HIA Regulations, and is targeted for completion within this fiscal year.

The IM/IT Strategy Committee (Appendix 3 – TOR) is an advisory committee that reports to the HIEC. They develop the three-year strategic plan for the Alberta EHR and additional e-Health initiatives and submit their recommendations to HIEC for adoption.

The EHR Sponsors Committee (Appendix 4 – TOR) is an advisory committee that reports to the HIEC. They are responsible for providing executive oversight to provincially funded e-Health initiatives including ANP enhancements. Under the EHR Sponsors Committee, there will be various project-based steering committees to address developments as needed. An example of a current steering committee is the Personal Health Portal Steering Committee.

The following are additional support service groups, who have specific knowledge or expertise, that provide information to the steering committees:

- Health Information Standard Council of Alberta (HISCA) mandate to oversee and coordinate the adoption, adaptation, and development of health information and technology standards for the Alberta healthcare system and to disseminate approved health information and technology standards to ensure these standards align with approved provincial standards, as well as national and international standards:
- Integrated Clinical Working Group is a multidisciplinary working group with the mandate to provide clinical perspectives and advice in the ongoing definition, development, implementation and operation of the EHR initiatives and other closely related activities (referred to as "EHR initiatives") who forwards recommendations regarding policy and strategy to the EHR Sponsors Committee when appropriate; and
- IM/IT Architecture Group is responsible for ensuring that the solutions designed and implemented through various projects conform to Alberta's overall architectural plan.

As the Alberta EHR evolves, new support service groups may be developed.

The structure for tri-lateral agreement includes the three partners AHW, AHS and Alberta Medical Association (AMA), and deals with two main initiatives: Physician Office Systems and Primary Care Networks.

2. Policy Management

AHW Policy Management:

Refer to Section E: Policy and Procedures Attachments in this PIA for supplemental information.

In accordance with the HIA and Regulations. AHW has developed two major policy documents:

- Information Management (IM) Policies Appendix 1; and
- Information Security Policy (ISP) Manual Appendix 5.

Policies are either derived from Ministerial Mandates, Department Directives, or Legislation. Policies are reviewed on a regular basis. Revisions and approvals to each policy are tracked within the Policy Directive or policy itself. When a revision, addition or removal of a policy is needed, the review and approval process will be done as required. Before policies are modified, added or removed, analysis must be performed to determine how such changes will impact other areas of AHW. Any governance section of a policy document will be reviewed and approved independently of the policies. ICAU takes the lead in the development of the policies within the two major policy manuals – IM and ISP. The approvals for these manuals are the responsibility of the ICAU Senior Manager, the Executive Director of the Information Management

Branch and ultimately the Assistant Deputy Minister for the Health System Performance & Information Management (HSPIM) Division and Executive Committee (EC).

The IM and ISP policies reflect a statement of intent and guidance by executive management to the organization as a whole regarding the commitment, ownership, responsibilities, processes, and other themes applicable to information management, such as privacy and security controls. Both sets of policies align with the HIA, which defines the behaviors, responsibilities and rules that AHW, as custodian, and its affiliates are required to follow. The Minister, Deputy Minister and all Executives are committed to managing properly and appropriately all health information in the custody or under the control of AHW.

Privacy and security requirements are also addressed in other AHW and Government of Alberta (GOA) documents, such as:

- AHW Guidance Notes for Access to Data Holdings (A2DH) Appendix 6.
- HIA Guidelines & Practices Manual available on AHW website: http://www.health.alberta.ca/documents/HIA-Guidelines-Practices-Manual.pdf.
- OIPC Privacy Impact Assessment (PIA) Guidelines available at the OIPC website: http://www.oipc.ab.ca/pages/home/default.aspx;
- GoA Privacy Information available on the *Freedom of Information and Protection of Privacy Act* (FOIP) website: http://foip.alberta.ca/index.cfm.
- GoA Oath of Office Public Service Act section 20(1), available from GoA/Queens Printer website: http://www.qp.gov.ab.ca/Documents/acts/P42.CFM
- AHW Information Security Handbook Appendix 7.
- AHW Information Security Classification Scheme Table Appendix 8.

Records Management:

The Minister for Service Alberta is responsible for the government-wide records management program under the *Government Organization Act* (Schedule 11) and the Records Management Regulation. Alberta government departments, boards and agencies are subject to the Records Management Regulation (AR 224/2001) and must adhere to the policies and guidelines established under this Regulation. The Alberta Records Centre, the Provincial Archives, and other secure sites effectively house the inactive records and coordinate disposition. The Alberta Records Management Committee (ARMC) endorses the International Standard on Records Management – ISO 15489 as a code of best practice for Alberta government departments, agencies, boards and commissions. This senior interdepartmental committee approves records retention and disposition schedules, provides advice to the Minister on the management of records in the custody or under the control of government organizations, and may also evaluate the implementation of the records management program. Within AHW, records and data taxonomy and disposition are the responsibility of the Corporate Records Management Office (CRMO).

The CRMO has developed an Enterprise Information Management (EIM) – Records Management (RM) Policy Framework (OIPC File # F5260). The EIM - RM Policy

Framework establishes principles, responsibilities, and requirements for managing AHW records to ensure compliance with GOA legislative obligations, as well as AHW and GOA policies, procedures, standards and best practices. The framework also creates an environment that will ensure the ongoing integrity, accessibility and usefulness of records. Currently the EIM initiative has addressed semi-structured and unstructured information. Future phases will address structured information (i.e. databases). Any prescribed health information within the custody or under the control of AHW is currently retained indefinitely.

The CRMO has also developed an EIM – Governance Policy Framework (OIPC File # F5260). The EIM Governance Policy Framework sets out AHW's commitment to the security, integrity, confidentiality and quality of the organization's information. This framework highlights the governing mechanisms by which to manage AHW's information assets.

ANP Policy Management:

Custodians who meet the eligibility requirements in the HIA and EHR Regulation can become authorized custodians and thereby access prescribed health information via the Alberta EHR. These eligibility requirements include signing an IMA with AHW. The EHR IMA incorporates by reference the IEP, which sets out the specific rules governing authorized custodians' use of prescribed health information via the Alberta EHR. The rules in the IEP work in conjunction with the HIA.

Only those affiliates of authorized custodians who meet eligibility requirements, as confirmed by the authorized custodian's AA, can become authorized users of the Alberta EHR and, therefore, can access prescribed health information via ANP. Custodians under the HIA have a legislative obligation to ensure their affiliates comply with their HIA-specific policies and procedures, including ensuring their authorized ANP users abide by the IEP.

ANP Records Management:

All electronic records in the Alberta EHR are retained according to the records management schedule that is applicable in the various repositories in which they are housed. The ANP does not retain any particular record as it is only a web-based portal application that enables the electronic viewing of health information.

Should authorized Alberta EHR users decide to print prescribed health information viewed via ANP to append to patients' medical records, those printed records are then governed by the records management schedule, professional standards and/or related business and legislative obligations (including the *Limitations Act* requirements) of the custodial body whose affiliates printed the information.

3. Training and Awareness

AHW Organizational Training:

The policy directives and statements contained in the IM and ISP policy documents apply to all AHW affiliates. These policy documents are intended to define the Operation Management (OM) requirements and responsibilities covering the management of the information and information systems within AHW's control. The IM and ISP policies are endorsed by all AHW executives, senior managers and managers who, in turn, are responsible for ensuring that all AHW affiliates understand their responsibilities to protect the confidentiality, integrity and availability of information in the custody or under the control of AHW.

AHW affiliates receive ongoing training that captures both HIA and Information Management (IM) policies and procedures to ensure they are knowledgeable regarding the application of privacy legislation to their jobs. This training will include topics such the HIA, FOIP, security standards and procedures, and retention and disposition of records, as well as training on specific topics which meets the needs of a unit/branch. Responsible program / business areas also have access to the comprehensive HIA Guidelines and Practices Manual⁵. All AHW employees must take the following mandatory training courses which are offered several times a year:

- Security Awareness The objective is to make employees aware of privacy and is intended to help them follow AHW-specific information security requirements. This in turn will reduce the risks associated with misuse of AHW information assets and equipment. AHW Executive supports the concept that security is a responsibility shared by everyone at AHW.
- HIA & FOIP General Awareness Overview of employee duties and obligations under each of the Acts.
- Managing Information @ Work Employees are required to have a consistent understanding of records management, IT security, access to information, and protection of privacy that can be applied in their day-to-day business activities.

AHW's Information Security Handbook is provided to all new staff and is also available via the AHW Intranet.

AHW has established a process to allow individuals to report privacy or security incidents or suspected incidents⁶. This ensures that AHW's responsibilities related to the protection of privacy and security are fulfilled, and to assist AHW in determining the cause of actual or suspected incidents so that any necessary steps are taken to prevent future occurrences.

_

⁵ Available online at AHW's public site: http://www.health.alberta.ca/about/health-legislation.html

⁶ Refer to PIA section B4.

The CRMO has developed brochure guides and "Fact Sheets" for AHW employees to ensure appropriate records management and disposition:

- Fact Sheet CRM Disposing of Paper Transitory Records
- Brochure Identifying & Disposing of Transitory Records
- Brochure Records Disposition & Retrieval
- Brochure Records Classification Guide

ANP Training:

Alberta EHR users receive training and change management support from the Alberta Netcare Deployment Team. The Alberta Netcare Deployment Team supports Alberta EHR users in planning, training and transition:

- Alberta Netcare Enrollment Line 1 (866) 756-2647 (toll free) or in Edmonton 780-642-4082 or email:health.ehrdeployment@gov.ab.ca.
- New Alberta EHR users will enjoy the learning package 'Getting Started' in ANP.
 It provides key information and tools that new users can use to integrate ANP
 into their busy workflow, such as Quick Reference Cards (QRCs) and e-Demos
 showing typical 'Getting Started' steps.
- Additional learning packages for PD and PIN are also available. Alberta EHR
 users can click Plan Your Learning to locate those resources that best match
 their ANP User Role and corresponding PD and/or PIN permission level.
- More experienced Alberta EHR users can search the Frequently Asked Questions (FAQ) for specific information, or link to the Learning Environment, where they can practice in a simulated ANP environment.
- Any Alberta EHR user may 'Submit a Question' and can expect a response within four business days.

Authorized custodians are also responsible for ensuring that they and their authorized affiliates (i.e. authorized ANP users) are aware and adhere to all of their administrative, technical and physical safeguards in respect of health information. This includes ensuring that their affiliates comply with their HIA-specific policies and procedures.

To assist custodians in Alberta, AHW has made available the following information that they can use when they establish their administrative safeguards:

HIA Training For Custodians and Stakeholders:

- Assessing the Impact
- Applying HIA
- General Awareness
- Health Information Act Guidelines and Practices Manual

4. Incident Response

AHW and ANP Incident Response:

The Provincial Reportable Incident Response Process (PRIRP) has been designed to ensure that all health stakeholders are aware of all possible threats to health data and how to respond to a suspected or real threat. The PRIRP is owned and managed by ICAU. For a detail description of how incidents are identified, investigated and managed please refer to:

 Appendix 9 – Provincial Reportable Incident Response Process Guide and Flowchart.

5. Access and Correction Requests

AHW Access and Correction Requests:

AHW administration of the FOIP policy legally delegates FOIP authorities and responsibilities to specific and appropriate positions within AHW. The FOIP Coordinator is responsible for the overall management of access to information (personal, general and correction) and protection of privacy under FOIP. Specific decision making powers, responsibilities and ability to act are delegated according to the FOIP delegation of authority instrument approved by the Minister (Appendix 10 - FOIP Administration and Delegation).

AHW administration of the HIA Policy states that the HIA Coordinator is responsible for the overall management of access to health information while the policy direction relating to the protection of health information under HIA is the responsibility of ICAU. The assignment of responsibility table under the HIA lists the duties, powers and functions assigned to individuals fulfilling specific positions (Appendix 11 - HIA Administration and Delegation).

ANP Access and Correction Requests:

HIA Part 2 sets out the rules that apply to individuals' rights to access their health information, including their prescribed health information accessible via the Alberta EHR. If an individual wants to know who has accessed his/her prescribed health information via the Alberta EHR, the individual must submit an access request to AHW specifically requesting a copy of his/her log. The form for making an access request along with guidelines may be viewed at the AHW public website: http://www.health.alberta.ca/documents/HIA-Request-Access-Form.pdf.

Individuals wishing to request changes be made to their information logs are directed to the custodial body or bodies responsible for having made that particular prescribed health information accessible via Alberta EHR. The appropriate custodial bodies will then assess whether or not the logs ought to be changed.

Section C: Project Privacy Analysis

1. Health Information Listing

ANP provides a patient-centric view of prescribed health information within the Alberta EHR. Prescribed health information is defined in section 4 of the HIA's EHR Regulation and currently includes the following types of information, all of which is in the custody and control of the authorized custodians whose data is considered the source of truth for that information:

AHS (Repositories)⁷

- TREP Transcribed Reports Repository (Edmonton)
- RREP Rural Report Repository
- CHRP EHR Index
- CHAP Capital Repository (houses Edmonton zone immunizations, home care summaries and ADT events)
- CHRLRP Calgary Laboratory Repository
- CHRDRP Calgary Diagnostic Imaging Text Report Repository
- CHRTRP Calgary Transcribed Report Repository (refer to OIPC File # H3035)
- LREP Laboratory Repository (Edmonton) which is owned by the Edmonton Zone Laboratory team and is used by Dynalife – their laboratory provider.

The repositories capture key clinical events at the point of care to provide health care providers with a more complete picture of a patient's encounters with the health system. Consequently these clinical systems provide a more comprehensive, up-to-date and accurate core medical information about a patient.

AHW (Registries and Provincial Applications)

- Provincial Person Directory (PD) (refer to OIPC File # H0565 and H0051)
- Provincial Client Registry (PCR) (refer to OIPC File # H1397)
- Alberta Provider Directory (ABPD) (refer to OIPC File # H0229)
- Delivery Site Registry (DSR) (no PIA completed on DSR as there is not individually identifying health information)
- Pharmaceutical Information Network (PIN) (refer to OIPC File # H3213)
- Chronic Disease Management (CDM) Information System (refer to OIPC File #'s H0375, H0771 and H1941)
- Enterprise Master Person Index (EMPI) (refer to OIPC File # H0272)
- Provincial Health Information Exchange (pHIE) (refer to OIPC File # H1556)

The registries provide timely and accurate reference information on clients, health services providers and facilities in the health care system. The provincial applications

⁷ Prior to consolidation into AHS, there were several clinical systems, including but not limited to, Sunrise, Meditech, Rural Medipatient and Mediscribe. These systems are integrated into the repositories that are listed. AHS has physical control of and maintains the repositories listed under this heading. AHS has committed to ensure that all PIA requirements are adhere to for the repositories.

provide authorized ANP users with business tools to enable them to complete their duties in the course of a health service event.

AHS operates the ANP, as well as the EMPI and pHIE applications, on behalf of AHW pursuant to an operating agreement. Operation of the ANP includes ensuring prescribed health information is accessible via the ANP from the various data sources that comprise the Alberta EHR.

Refer to:

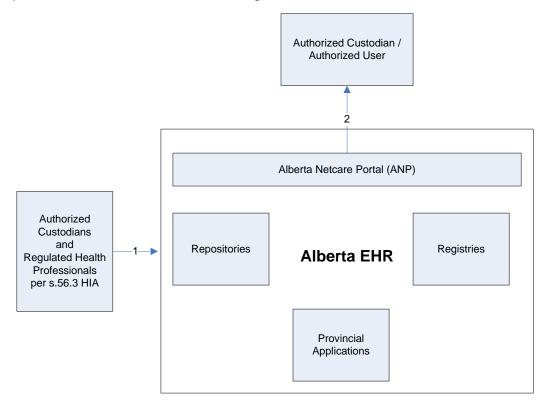
- OIPC File # H1124 Alberta Netcare EHR Portal 2006.
- Appendix 12 Data Availability Table.
- Appendix 13 Current Data Sources and Repositories

Please note that due to the recent HIA amendments which formally acknowledge the Alberta EHR, the stated legal authorities in existing accepted PIAs that pertain to the Alberta EHR will have to be updated.

Information Flow Analysis

The ANP is a key component of the Alberta EHR in that it is the exclusive entry point/viewer of prescribed health information. Please note this PIA addresses the ANP in isolation and does not pertain to any specific information flows. Rather, this PIA addresses the ANP application in its role as gateway to all authorized viewings of all and any prescribed health information (i.e. authorized uses of that information under HIA). ANP is not used to populate and maintain the data repositories that comprise the Alberta EHR. Project-specific PIAs will address the use of specific types of prescribed health information by specific authorized custodians as well as the maintenance and connectivity of the data repositories, provincial applications, and registries that comprise the Alberta EHR.

Component # 1 – Information Flow Diagram:



NOTES:

- The diagram depicted above is not intended to represent information flows and technical connectivity between and among systems comprising the Alberta EHR (i.e. within the box entitled Alberta EHR in the above diagram).
- The initial collection of prescribed health information occurs by the authorized custodians and regulated health professionals depicted in Flow #1 in the diagram as authorized by Part 3 of the HIA.

Component #2 – Information Flow Table:

Flow #	Description	Type of Information	Purpose	Legal Authority
1	Regulated health professionals and authorized custodians (s.56.3 HIA)	Prescribed health information (defined in s.56.1(c) HIA and s.4 EHR Regulation). Refer to PIA section C1.	In accordance with s.56.3 HIA and s.5 EHR Regulation, and as directed by the Minister and/or health professional bodies, in conjunction with ministry and committee directives, authorized custodians or regulated health professionals may make prescribed health information accessible via the EHR for the benefit of the public and provision of health care in Alberta.	Authority to make information accessible via Alberta EHR (i.e. use): s.56.3 HIA; Duty to consider expressed wishes of individuals in doing so: s.56.4 HIA. Alberta EHR IMA.
			In making prescribed health information accessible via the Alberta EHR, these authorized custodians and regulated health professionals must also, in accordance with s.56.4 HIA, consider the expressed wishes of individuals in deciding how much prescribed health information to make accessible. (See Appendix 19.)	
			The databases and repositories from which information is made accessible via the Alberta EHR communicate with each other (i.e. pHIE or direct from source systems) to ensure all data remains as accurate as possible at all times. The details and specific legal authorities pertaining to specific prescribed health information repositories and related applications should all be addressed in their respective project-specific PIAs.	
2	Authorized custodians (defined in s.56.1(b) HIA) view ("use" per s.56.5 HIA) prescribed health information for an authorized purpose under	Prescribed health information (defined in s.56.1(c) HIA and further described in s.4 EHR Regulation). Refer to PIA section C1.	Authorized custodians (and through them their affiliates that are authorized users of the Alberta EHR) can use prescribed information only for those purposes authorized by the HIA. Authorized custodians referred to n s.56.1(b)(i) of the HIA may	Authority to use prescribed health information: s.56.5 HIA and, depending on type of authorized custodian, corresponding underlying authority in s.27

Flow #	Description	Type of Information	Purpose	Legal Authority
	HIA.		use prescribed health information accessible via the Alberta EHR for any purpose authorized by section 27 of HIA. (Section 56.5(1)(a) HIA.) Authorized custodians referred to in s.56.1(b)(ii) of the HIA may use prescribed health information accessible via the Alberta EHR, and that is not otherwise in the custody or control of that authorized custodian only for a purpose authorized by (i) section 27(1)(a), (b) or (f), or (ii) section 27(1)(g), but only to the extent necessary for obtaining or processing payment for health services. (Section 56.5(1(b).)	HIA. As discussed in the Alberta Netcare Portal Permission Matrix in Appendix 16, authorized custodians' authorized users are further restricted to what prescribed health information they can access (i.e. use) by user role, etc. Alberta EHR IMA.

2. Notice

Viewing/accessing prescribed health information via the ANP is a use of that information as per HIA section 56.5. This use of individually identifying prescribed health information via ANP does not require individual consent (i.e. notification) of the patient who is subject of the information; however, section 56(4) of HIA requires authorized custodians or regulated health professionals to consider the individuals' expressed wishes in deciding how much prescribed health information to make accessible via Alberta EHR. Again, ANP is view-only and is *not* used to populate or otherwise make prescribed health information accessible via the Alberta EHR.

3. Consent and Expressed Wishes

In order to respect the expressed wishes of individuals to limit access to their prescribed health information, information accessible via ANP may be masked. For Albertans who wish to limit the use of their prescribed health information, authorized custodians or regulated health professionals (i.e. those with authority under s.56.3 HIA to make information accessible via the Alberta EHR) have a mechanism to mask health information called *Global Person-Level Masking* (GPLM). When an authorized custodian attempts to access prescribed health information about an individual who has made a masking request, only the first and last name, date of birth, gender and personal health number of that individual will be visible to that authorized custodian via ANP.

Please refer to Appendix 19 for the following GPLM documents:

- FAQs
- Application for GPLM
- Authorization to Rescind GPLM

In addition, members of the public can also obtain information on the GPLM process at this link http://albertanetcare.ca/11.htm, which is specifically found under the Privacy and Security heading under the Alberta Netcare Information section of the Alberta Netcare website.

How GPLM Works

When a mask has been applied, all of the prescribed health information contained in the patient's EHR will not automatically be displayed. The authorized ANP user sees an indicator that the data is masked. This user must then decide if this data is 'need to know' and, if it is, to unmask the data. The user must select the reason for the unmasking. This is referred to as 'breaking the glass' before the prescribed health information can be viewed. There are six possible reasons for unmasking:

- patient consent,
- · direct patient care/clinical need,
- medical emergency,
- public health follow-up,
- · authorized release of patient information, and
- as required by law.

The unmasking of health information is logged and subject to auditing, as are all viewings through ANP.

Requesting the Mask

Individuals wishing to request GPLM must contact an authorized custodian or regulated health professional with whom they have a current care relationship⁸. The party receiving the request must complete the GPLM application form in conjunction with the individual and then submit the application to AHS for processing.

Before submitting the application, the authorized custodian or regulated health professional must discuss the consequences of applying and rescinding a mask with the individual. Further, there may be circumstances in which a party is unable to authorize an individual's information to be masked - for example, if masking that information could pose a threat to public health and safety.

Rescinding a Mask

-

⁸ Note - while AHW is a custodian under HIA, AHW does not participate in ANP as a health care provider. AHW does not have a current care relationship with Albertans who are asking for their information to be masked so is not in a position to consider the best way to respond to an individual's request. AHW provides direction on who to contact in AHS to request the mask. AHS is AHW's service provider in this regard.

An individual may also request that a mask be rescinded by contacting an authorized custodian or regulated health professional. A request to rescind a mask may also be initiated by a health services provider if he or she becomes aware of circumstances that affect an individual's eligibility for GPLM. In this case, authorized custodians/regulated health professionals or their delegates will make every attempt to inform the individual of their decision prior to removing the mask. Applications to rescind masks must also be submitted to AHS for processing.

Contacts

As information manager of the Alberta EHR, AHW is responsible for establishing and communicating the formal GPLM process. The AHW HIA Help Desk⁹ offers support to individuals who request their information be masked by providing information about the masking process and the authorized custodian's or regulated health professional's role in the process. The AHW HIA Help Desk will follow up should the individual have difficulty engaging in the masking process; however, per footnote 7 above, AHS provides the actual masking service on behalf of AHW. AHW is responsible to enable and maintain the setting of the mask in ANP. All complete GPLM forms are handled by the AHS Edmonton Zone Patient Information Services which is responsible for the 'technical' aspects of adding and removing masking flags on behalf of AHW. AHS administers GPLM for AHW in accordance with operating agreements. Also refer to section C5 of this PIA.

4. Data Matching

Not applicable. The ANP enables viewing of prescribed health information and does not meet the definition of data matching in section 1(1)(g) of the HIA.

5. Contracts and Agreements

AHS provides operational support to AHW for ANP pursuant to an operational agreement.

AHW and AHS technical support is partially provided by third party vendors. For example, although the majority of the ANP technical support is provided by AHS staff, some additional ANP technical support is provided by a third party vendor (Orion). The agreements between the vendors and the signing custodians make the vendors affiliates. These agreements include security, access and confidentiality clauses that obligate the vendors to adhere to legislation, standards, policies and information

⁹ The Health Information Act (HIA) Help Desk can be reached from 8:15 a.m. to 4:30 p.m. (Monday to Friday, excluding statutory holidays) at 780-427-8089, or toll free in Alberta by dialing 310-0000 then 780-427-8089; email hiahelpdesk@gov.ab.ca

management requirements of either custodian. Any relevant third party vendor agreements should already be addressed in project specific PIAs.

6. Use of Health Information Outside Alberta

Only authorized custodians and their authorized users can access prescribed health information via the Alberta EHR. The HIA and regulations define authorized custodian and the eligibility requirements to become one. Currently, all authorized custodians are either regulated health services providers or Alberta-based organizations or entities. Since the ANP is web-based, authorized ANP users may access the Alberta EHR while outside the province. Authorized custodians who access (i.e. use) prescribed health information while outside of Alberta are responsible to ensure that they have proper legal authority to do so.

Section D: Project Privacy Risk Mitigation

1. Access Controls

Section 3 of the new HIA EHR Regulation sets out detailed eligibility requirements whereby custodians may become authorized custodians and thereby, access prescribed health information via Alberta EHR. This section essentially codifies pre-HIA amendment practices whereby custodians became authorized to access information via the Alberta EHR (hence why pre-HIA amendment custodians with this access automatically become authorized custodians per s.3(3) of the EHR Regulation).

Per section 3(d) of the EHR Regulation, all authorized custodians must sign an IMA with AHW. Only then are these authorized custodians allowed to register themselves or their affiliates as authorized users and be given a login ID. Access guidance and instruction is also provided via the ANP Access Administrator Guide. An AA is the primary contact with AHW at the facility/site of an authorized custodian. Within each authorized custodian's organization, only those affiliates who meet eligibility requirements, as confirmed by the authorized custodian's AA, become authorized users of the Alberta EHR (and therefore can access prescribed health information via ANP).

The amount and type of prescribed health information available via ANP to authorized custodians and their authorized ANP users is read-only and based on user role permissions, as established in the ANP Permission Matrix. (Refer to Appendix 20.) This means that access permissions and other security credentials are set up so that users have enough information to do their jobs, while ensuring that information is accessible on a 'need-to-know' basis. (Refer to Alberta Netcare Portal Permission Matrix in Appendix 16).

Roles are well-defined for the ANP application and are divided into three categories: Admin, Pharmacy and Clinical. AHW developed the ANP Permission Matrix in collaboration with AHS via the Health Sector Security Working Group. Prior to its

implementation, it was reviewed and approved by the Electronic Health Record Data Stewardship Committee (EHRDSC).

The ANP is a web-based application delivered via a secure browser interface. Access is via the Internet and can be from within a secure network (i.e. AHS facility) or from remote sites (community facilities). Alberta EHR users accessing ANP within a secure zone do not require "two factor" authentication, as they have met the pre-established AHW MCR and only have to use their ANP username and password. All Alberta EHR users from remote sites such as private providers (including long term care organizations), physician offices, and pharmacies are required to use "two factor" authentication using either a hard or soft token along with their ANP username and password.

Section 3(c) of the EHR Regulation and AHW Department standards also require authorized custodians from remote sites such as private providers (including long term care organizations), physician offices, and pharmacies to conduct a p-ORA which reviews and ensures that administrative, technical and physical security controls are in place to mitigate risks of accidental or malicious access to prescribed health information, including:

- All authorized ANP users must utilize a 'User Name' and 'Password' to enable ANP access. The 'User Name' and 'Password' validate that the users are who they say they are (authentication).
- All Alberta EHR users must be aware of the Terms of Use and Disclaimer for the ANP.

The security controls used to protect information viewable through ANP are based on international standards and best practices. All user access to ANP is logged and access logs are audited monthly. Section 7 of the EHR Regulation now requires AHW as information manager of the Alberta EHR to conduct such monthly audits. All electronic messages are encrypted. Network security controls include the use of firewalls and intrusion detection tools to alert the appropriate personnel of any unusual activity.

Section 6 of the EHR Regulation also sets out all custodians' logging requirements in respect of their electronic health record information systems, as such systems are now defined in s.1(b) of the EHR Regulation. Section 6(2) of the EHR Regulation states this section of the regulation applies only to electronic health record information systems established after the coming into force of this section; however, pre-EHR Regulation custodians with access to the Alberta EHR were and continue to be bound by equivalent policies, practices, and information manager agreements.

AHW has implemented the provincially reportable incident response process that has been designed to ensure that health stakeholders are aware of all possible threats to health data and how to respond to a suspected or real threat. This process provides guidance to all organizations as to the definition of what AHW considers a valid threat to health data.

The HIA imposes fines for anyone who knowingly collects, uses, or discloses health information or who gains or attempts to gain access to health information in contravention of the Act. Individuals who breach privacy and access rules could also be subject to criminal charges, fines, and disciplinary measures within their licensing or professional organization. The recent amendments to the HIA include an additional penalty in s.107(6.1) for any person who uses prescribed health information in contravention of s.56.4 HIA (expressed wishes provision).

2. Privacy Risk Assessment and Mitigation Plans

Privacy Risk	Description	Mitigation Strategies	Reference
Unauthorized use of	Gaining unauthorized	Access Control & Monitoring:	
prescribed health information	access to systems or	 Restricting access to patient information based on 	Alberta Netcare Portal Permission Matrix
by internal or authorized	networks.	the user's role and profession.	
parties	Chanain a suntana	Every ANP user has a unique user ID and	Albert Netcare User Registration Form
	Changing system privileges without	password. Each user is accountable for their access to ANP.	
	authorization.	 Logging all user-initiated activity. Audits are done 	Alberta Electronic Health Record Regulation s. 7
	authorization.	routinely, randomly and on the request of patient	- Alberta Electronic Fleatin Necora Regulation 3. 7
	Disclosing authentication	or health care provider.	
	information	Training:	
		 Custodian provides ongoing security and HIA/FOIP 	Organizational specific processes
	Misusing/disclosing ANP	awareness training to affiliates.	■ HIA s. 62
	EHR information to	The ANP Deployment Team provides Alberta	 https://ab-ehr-learningcentre.albertanetcare.ca/
	commit fraud.	Netcare training to Alberta EHR users. There is a	
		Learning Centre for authorized ANP users.	
		User Obligations: Fines are in place in the HIA where an individual	■ HIA s. 107
		knowingly collects, uses, discloses or creates	• піа 5. 107
		health information in contravention of the Act.	
		Increased fines for using prescribed health	
		information in contravention of s.56.4 HIA	
		(expressed wishes).	
		 Health care providers face fines and sanctions 	 Organizational specific processes
		from their licensing and/or professional	
		organization if they use health information	
		inappropriately.	
		 Terms of Use and Disclaimer available from the ANP Login box. 	http://www.albertanetcare.ca/233.htm From a secure zone – Alberta Network log-in screen:
		ANP LOGITI BOX.	https://portal.albertanetcare.ca/ab/NetcareLogin.htm
			Remotely via the internet with two-factor authentication
			(fob) – network log-in screen (Term and Use Disclaimer on
			next log-in screen):
			https://portal.albertanetcare.ca/ab/NetcareLogin.htm
			and then via the actual Alberta Netcare log-in screen:

Privacy Risk	Description	Mitigation Strategies	Reference
·	Lack of submitted PIAs on AHS (Repositories) to the OIPC for review, comment and subsequent acceptance	AHS is currently in the process of consolidating the information of PIAs captured in the former regions repository PIAs as they work to submit an AHS (Repositories) PIA.	https://portal.albertanetcare.ca/ab/NetcareLogin.htm PIA
Unauthorized collection/use/disclosure of health information by external parties	External party gains access to an authorized ANP user's password and user name. Hacking into ANP. Misusing prescribed	 Access control & Monitoring: In accordance with HIA and regulations, only authorized custodians and their affiliates can become authorized ANP users. No external parties can gain access to the Alberta EHR via ANP unless they gain access to an authorized ANP user's password and user name. Restricting access to prescribed health information based on the user's role and 	 Netcare IMA p-ORA Alberta Netcare Portal Permission Matrix Albert Netcare User Registration Form
	health information to commit fraud.	 profession. Every ANP user has an obligation to secure their authentication credentials. Each user is accountable for their access to ANP. Logging all user-initiated activity. Audits are done routinely, randomly and on the request of patient or health care provider. Assessments: Privacy and security assessments are conducted on potential ANP users. 	 Netcare IMA System Logging PIAs p-ORA's
	Lack of submitted PIAs on AHS (Repositories) to the OIPC for review, comment and subsequent acceptance	 Network Control: Adequate network security controls are implemented such as intrusion prevention system, and firewalls to prevent external attacks. AHS is currently in the process of consolidating the information of PIAs captured in the former regions repository PIAs as they work to submit an AHS (Repositories) PIA. 	 Alberta Netcare Network Architecture PIA

Privacy Risk	Description	Mitigation Strategies	Reference
Loss of integrity of	Unauthorized changes in	 Data source providers (i.e. authorized custodians 	Provincial Change Management Process
information	source system.	whose data repositories comprise the Alberta	 Organizational specific processes
		EHR) are required formally to signoff that	
	Unauthorized	presentation of their data via ANP is correct. This	
	interception of	includes both at initial implementation and	
	information in transit.	whenever a change is made to their interface and	
		with each ANP release. They are responsible for	
		the integrity of data submitted accessible within	
		Alberta EHR via ANP.	Dan in siel Matura de Daniera
		To eliminate the possibility of someone intercepting confidential health data all data	Provincial Network Design
		intercepting confidential health data, all data transfers outside of the secure network will be	
		encrypted. All portal access will be by secure HTTP	
		(HTTPS).	
		Access Control:	
		 Only authorized system administrators can access 	Administrator Access Management
		the ANP infrastructure.	
		 Only authorized users are allowed access to ANP. 	Alberta Netcare Portal User Registration Form
		 Remote authorized ANP users must use two factor 	
		authentications to access ANP.	
		 ANP is view only and has role-based permissions. 	Alberta Netcare Portal Permission Matrix
Loss, destruction or loss of	Computer virus could be	 Adequate network security controls are 	Alberta Netcare Network Infrastructure
use of prescribed health	introduced.	implemented such as intrusion prevention	
information		system, and firewalls.	
	Damage to or loss of IT	 To eliminate the possibility of someone 	Provincial Network Design
	infrastructure.	intercepting prescribed health information, all	
		data transfers outside of the secure network will	
		be encrypted. All ANP access will be by secure	
		HTTP (HTTPS).	Alle oute Net coue Network Aughitecture
		Fully redundant infrastructure, with automated failurer and recovery.	Alberta Netcare Network Architecture
		failover and recovery.All prescribed health information is stored in	Administrator access as per organizational specific
		secure repositories	processes
Unauthorized or	Third party vendor	Third party vendors must sign an agreement that	Vendor agreements
inappropriate collection/use	accesses prescribed	include security, access and confidentiality clauses	Terradi agreements
or disclosure by a contractor	health information for	that obligate the vendor to adhere to legislation,	
or business partner	purposes that are	standards, policies and information management	

Privacy Risk	Description	Mitigation Strategies	Reference
	outside the legal agreement.	requirements of either custodian. By signing these agreements the vendor becomes an affiliate of the signing custodian.	
	Misusing prescribed health information to commit fraud.	Access control & Monitoring: Users are only allowed to view data for which they require access.	Alberta Netcare Portal Permission Matrix
		 Every ANP user has a unique user ID and password. Each user is accountable for their access to ANP. 	Alberta Netcare Portal User Registration Form
		 Logging all user-initiated activity. Audits are done routinely, randomly and on the request of patient or health care provider. 	System LoggingInfrastructure Logging
		Training: Custodian provides ongoing security and HIA/FOIP awareness training to affiliates.	Organizational specific processesHIA s. 62
	Lack of submitted PIAs on AHS (Repositories) to the OIPC for review, comment and subsequent acceptance	AHS is currently in the process of consolidating the information of PIAs captured in the former regions repository PIAs as they work to submit an AHS (Repositories) PIA.	• PIA

The AHW Information Compliance and Access Unit (ICAU) – Security Team completed a Threat and Risk Assessment (TRA) on the ANP (refer to Appendix 20). The TRA utilizes Information Risk Assessment Methodologies (IRAM) that identifies potential privacy risks and the compensating security safeguards to mitigate the identified risks.

3. Monitoring

In accordance with Provincial Logging and Audit Standards, system logging provides a per user access log of all activity on ANP and will record who accessed what data and the time each user logs-in.

In accordance with s.56.6(1), all accesses to (i.e. uses of) prescribed health information pursuant to s.56.5 HIA must be logged. Access to a patient's prescribed health information must be logged and be subsequently displayed in the appropriate fields in the audit reports described below. Per section 6 EHR Regulation, the following data elements must also be logged each time individually identifying information is accessed by an authorized custodian or their authorized users via an electronic health record information system:

- <u>User ID or application ID associated with an access</u>: This is a unique identifier for a user or application. This data element should be logged once during an access to a patient's record.
- Name of user or application that performs an access: This is the full name of a user that accesses a patient's record. In the case of system-to-system communication, this is the application name. This data element should be logged once during an access to a patient's record. For instance, if a user accesses a patient's record in PIN, the user's name should be logged once as long as the PIN session for that access stays alive no matter how long that session stays alive. This line of thought is used to describe logging requirements for subsequent data elements. If it is possible to derive the name of the user or application that performs the access from the user ID, then this data element should not be logged.
- Role (or profession or occupation) of a user who performs an access: This
 refers to the job function of a user performing an access. For instance, physician,
 pharmacist, nurse, etc. This data element should be logged once per access to a
 patient's record.
- <u>Date of access</u>: This refers to the day, month and year that a user or application performs an access. This should be logged once per access.
- <u>Time of access</u>: This refers to the hour, minute and second that an access is performed. This data element is logged each time an action is performed on a patient's record during an access. The time of access must be synchronized with local time.

- Actions performed by a user during an access: This may include one or a
 combination of the following: create, view, update or modify, delete, patient
 search, copy, print, etc. These data elements must be logged each time an
 action corresponding to any of the above is performed on a patient's record by a
 user during an access.
- Name of facility or organization of access: This data element should be logged once per access to a patient's record.
- <u>Display Screen Number or Reference</u>: This refers to the user interface or application that was used by a user during an access, for instance, PIN. This data element should be logged once per access.
- Stakeholder unique Identifier: This data element should be logged once per access to a patient's record. The unique identifier does not have to be part of the logs as long as it can be displayed in the audit report when needed. Example of unique identifier includes medical record number (MRN) and personal health number (PHN). One of these identifiers needs to be displayed in the audit report as two or more patients whose records have been accessed can have similar names.
- <u>Stakeholder name</u>: This is the name of the patient whose information is being accessed. This field should be logged once per access to a patient's record. If it is possible to derive the stakeholder name from the PHN without affecting the efficiency of the logging application, then, stakeholder name should not be logged.

As indicated, AHW is the Alberta EHR information manager (s.2 HIA EHR Regulation) and has established the Provincial Logging and Audit Standard for all Electronic Health Record Information Systems, which also includes ANP (refer to Appendix 21). Section 7 of the EHR Regulation requires the information manager of the Alberta EHR to conduct an audit each month of the Alberta EHR information logs. The Provincial Logging and Audit Standard captures the data elements that have been listed above each time individually identifying information is accessed by an authorized custodian or their authorized users via ANP.

AHW conducts both random monthly audits from the generated user access log of all ANP activity and on demand when requested by a custodian. Individuals can also submit an HIA Access Request to the AHW FOIP office to obtain a copy of an audit log, for a specific period of time, so that they may find out who has been accessing their EHR.

Custodians or individuals that suspect that their EHR has been inappropriately accessed, can raise this concern with AHW, which would trigger a breach investigation

using the Provincial Reportable Incident Response Process (PRIRP), found in Appendix 9.

4. PIA Compliance

Section 8(3) of the HIA Regulation stipulates that custodians must periodically assess their administrative, technical and physical safeguards. One of those administrative safeguards includes ensuring compliance with section 64 of the HIA. AHW strives for PIA compliance with section 64 of the HIA. To this end, the Electronic Health Records Delivery Services business unit will consult with the AHW Privacy Team as soon as any changes are anticipated to the ANP. The AHW Privacy Team will then identify any new privacy impacts that need to be addressed and determine if a PIA amendment is required and, if so, what form it should take and will submit it to the OIPC for review, comment and subsequent acceptance.

Section E: Policy and Procedures Attachments

Appendix – denoted as "A" Page – denoted as "P"

	General Privacy Policies/Procedures				
Topic	Description Mitigation Strategies Reference				
Privacy Accountability	This is a broad policy that enables privacy roles and accountability within your organization. Sometimes called a privacy charter, this policy does not provide detailed work instructions, but rather sets out responsibilities and commitments	 Where privacy fits into your organizational structure? IM Policy 001 – Compliance. IM Policy 002 – Delegation of Oversight. 	• A1, P2 • A1, P4		
	in relation to privacy.	2. Who is responsible for privacy, including who is responsible for responding to privacy complaints?			
		 IM Policy 002 – Delegation of Oversight. 	■ A1, P4		
		 FOIP Administration and Delegation. 	• A10		
		 HIA Administration and Delegation. 	■ A11		
		3. Who is responsible for information security?			
		■ ISP Manual ¹⁰ - Governance Section.			
		 ISP Policy Directive 1.0 – Organizational Security. 	■ A5, P7		
		4. Commitment to protect confidentiality and to collect, use and disclose health information in a limited manner?			
		 IM Policy 001 – Compliance. 	■ A1, P1		
		 IM Policy 003 – Duty to Collect, Use and Disclose Health Information with the Highest Degree of Anonymity Possible and in a Limited Manner. 	■ A1, P7		
		 IM Policy 005 – Collection of Health Information. 	■ A1, P5		
		 IM Policy 008 – Use of Health information. 	■ A1, P18		
		 IM Policy 011 – Disclosure of Information Process. 	■ A1, P22		
		 IM Policy 013 – Disclosure Notification 	■ A1, P29		
		 IM Policy 023 – Privacy Impact Assessments (PIAs). 	■ A1, P54		

-

¹⁰ AHW Security Polices was submitted with Electronic Health Record (EHR) – Release 1.0 PIA (Part A) OIPC File # H0222. These policies are currently being refreshed and when complete will be re-submitted to OIPC with the next PIA.

	General Privacy Policies/Procedures			
Topic Description Mitigation Strategies Referen				
•	-	 IM Policy 024 – PIAs for Disclosure for Health System Purposes. 	■ A1, P58	
		 IM Policy 025 – PIAs for Data Matching. 	A1, P60	
		 IM Policy 026 – PIAs for Data Matching for Research Purposes. 	A1, P 64	
		 IM Policy 027 – Access to Data Holdings Process. 	A1, P67	
		 IM Policy 028 – Privacy Breaches 	A1, P69	
		 ISP Policy Directive 3.0 – Personnel Security. 	 A5, P18 	
		 ISP Policy Directive 5.0 – Communications and Operations Management. 	■ A5 P27	
		 ISP Policy Directive 6.0 – Authentication and Access Control. 	 A5, P42 	
		 ISP Policy Directive 8.0 – Legislative Compliance Security Policies 	 A5, P63 	
		GOA Oath of Office		
		5. Commitment to maintain accuracy of health information?		
		■ IM Policy 001 – Compliance.	A1, P1	
		 IM Policy 023 – Privacy Impact Assessments (PIAs). 	A1, P54	
		 IM Policy 024 – PIAs for Disclosure for Health System Purposes. 	■ A1,58	
		 IM Policy 025 – PIAs for Data Matching. 	A1, P60	
		 IM Policy 026 – PIAs for Data Matching for Research Purposes. 	A1, P64	
		 IM Policy 027 – Access to Data Holdings Process. 	A1, P67	
		 IM Policy 028 – Privacy Breaches. 	A1, P69	
		 ISP Policy Directive 5.0 – Communications and Operations Management. 	■ A5, P27	
		 ISP Policy Directive 6.0 – Authentication and Access Control. 	 A5 P42 	
		 ISP Policy Directive 8.0 – Legislative Compliance. 	 A5 P63 	
		■ ISP Policy Directive 9.0 – Risk Assessment.	■ A5, P66	
		6. Commitment to provide privacy training and awareness to employees?		
		■ IM Policy 001 – Compliance.	■ A1, P1	
		 ISP Policy Directive 3.0 – Personnel Security. 	■ A5, P18	
		7. Commitment to maintain technical and administrative safeguards to protect health information?		
		■ IM Policy 001 – Compliance.	A1, P1	
		 ISP Policy 1.0 – Organizational Security. 	A5, P7	

	General	Privacy Policies/Procedures			
Topic	Topic Description Mitigation Strategies Reference				
·		 ISP Policy Directive 6.0 – Authentication and Access Control. ISP Policy Directive 7.0 – Systems Development and Maintenance. ISP Policy Directive 8.0 – Legislative Compliance. ISP Policy Directive 9.0 – Risk Assessment. 8. Right of access to health information and right to request corrections?	 A5, P42 A5 P54 A5, P63 A5, P66 		
		 IM Policy 001 – Compliance. IM Policy 002 – Delegation of Oversight. IM Policy 004 – Duty to Assist Individual's Right of Access to Information. 	A1, P1A1, P4A1, P9		
		 9. Schedule for periodic review of privacy policies? IM Policy 001 – Compliance. ISP Policy Directive 1.0 – Organizational Security 	A1, P1A5, P7		
Access to Health Information	Process and timeframes for responding to formal requests from individuals for access to their own health information.	 IM Policy 001 – Compliance. IM Policy 002 – Delegation of Oversight. IM Policy 004 – Duty to Assist Individual's Right of Access to Information. 	 A1, P1 A1, P4 A1, P8 		
		 FOIP Administration and Delegation. HIA Administration and Delegation. AHW HIA Guidance & Practices Manual. 	A10A11AHW Public website		
Correction Requests	Process and timeframes for responding to individuals who ask you to correct their health information.	 IM Policy 001 – Compliance. IM Policy 002 – Delegation of Oversight. IM Policy 004 – Duty to Assist Individual's Right of Access to Information. 	A1, P1A1, P4A1, P7		
		 HIA Helpdesk AHW HIA Guidance & Practices Manual. 	AHW Public websiteAHW Public		
Training, Awareness & Sanctions	Privacy training program for employees and others that will have access to health information in your custody.	 IM Policy 001 – Compliance. IM Policy 003 – Duty to Collect, Use and Disclose Health Information with the Highest Degree of Anonymity Possible and in a Limited Manner. 	website • A1, P1 • A1, P7		

	General Privacy Policies/Procedures				
Topic	opic Description Mitigation Strategies				
•		AHW HIA Guidance & Practices Manual.	 AHW Public website 		
Collection of Health Information & Notice	Acceptable reasons for collecting health information, which should include statutory authority, under the HIA or other relevant legislation.	 IM Policy 001 – Compliance. IM Policy 003 – Duty to Collect, Use and Disclose Health Information with the Highest Degree of Anonymity Possible and in a Limited Manner. IM Policy 005 – Collection of Health Information. IM Policy 006 – Collection of Personal Health Number (PHN). IM Policy 007 – Collection Notice. AHW HIA Guidance & Practices Manual. 	 A1, P1 A1, P7 A1, P12 A1, P14 A1, P16 AHW Public website 		
Use of Health Information	Acceptable uses of health information in your organization.	 IM Policy 001 – Compliance. IM Policy 003 – Duty to Collect, Use and Disclose Health Information with the Highest Degree of Anonymity Possible and in a Limited Manner. IM Policy 008 – Use of health Information. 	• A1, P1 • A1, P7		
Disclosure of Health Information	Reasons why your organization discloses health information to other organizations or persons.	 IM Policy 001 – Compliance. IM Policy 003 – Duty to Collect, Use and Disclose Health Information with the Highest Degree of Anonymity Possible and in a Limited Manner. 	• A1, P1 • A1, P7		
		 IM Policy 009 – Consent Based Disclosure. IM Policy 010 - Exceptions to Consent Based Disclosure. IM Policy 011 – Disclosure of Information Process. IM Policy 012 - Third Party Disclosure. IM Policy 013 – Disclosure Notification. IM Policy 014 – Disclosure to Police Services. IM Policy 015 – Disclosures to Prevent Fraud or Abuse of Health Services. IM Policy 016 – Disclosure to Prevent or Limit Fraud or Abuse of Health Services by Health Services Providers. 	 A1, P20 A1, P23 A1, P25 A1, P27 A1, P29 A1, P32 A1, P34 		
Research	How your organization handles research, requests from researchers under Sections 48-56 of the HIA.	 IM Policy 017 – Disclosure to protect public health and safety. IM Policy 019 – Research. IM Policy 026 – Privacy Impact Assessments for Data Matching for Research Purposes. 	A1, P40A1, P45A1, P64		
Third-Parties	How you ensure that third parties, which include contractors and information managers, protect your organization's health information.	 IM Policy 001 – Compliance. IM Policy 003 – Duty to Collect, Use and Disclose Health Information with the Highest Degree of Anonymity Possible and in 	A1, P1A1, P7		

	General Privacy Policies/Procedures				
Topic	Description	Mitigation Strategies	Reference		
Privacy Impact Assessments (PIAs)	Circumstances that trigger your organization to conduct privacy impact assessments.	 a Limited Manner. IM Policy 018 – Contracting. IM Policy 020 – Information Manager Agreements. IM Policy 001 – Compliance. IM Policy 023 – Privacy Impact Assessments. IM Policy 024 – Privacy Impact assessments for Disclosure for Health System Purposes. IM Policy 025 – Privacy Impact Assessments for Data Matching. IM Policy 026 – Privacy Impact Assessments for Data Matching for Research Purposes. 	 A1, P43 A1, P47 A1, P1 A1, P54 A1, P58 A1, P60 A1, P64 		
Records Retention & Disposition	How long you keep records containing health information and what you do with them once they are no longer needed.	 IM Policy 001 – Compliance. EIM – Records Management Policy Framework. EIM – Governance Policy Framework. GOA – Records Management 	 A1, P1 OIPC File # F5260, A6 OIPC File # F5260, A7 Records Management Regulation - AR 224/2001; and Government Organization Act - Schedule 11 		
Information Classification	Information should be protected at a level commensurate with its sensitivity and the risks it faces.	 IM Policy 001 – Compliance. IM Policy 021 – Provincial Courier. AHW Information Security Classification Scheme Table. AHW Information Security Handbook. 	A1, P1A1, P49A8A7		
Risk Assessment	New risks to the confidentiality, integrity and availability of health information may arise over time as technology and business processes evolve. This is your policy for conducting periodic risk assessments to assess the effectiveness of your privacy policies.	 IM Policy 001 – Compliance. IM Policy 023 – Privacy Impact Assessments. IM Policy 024 – Privacy Impact assessments for Disclosure for Health System Purposes. IM Policy 025 – Privacy Impact Assessments for Data Matching. IM Policy 026 – Privacy Impact Assessments for Data Matching for Research Purposes. ISP Policy Directive 9.0 – Risk Assessment. 	 A1, P1 A1, P54 A1, P58 A1, P60 A1, P64 A5, P66 		
Physical Security of Data & Equipment	The physical and administrative measures you take to secure health information in paper and electronic form. This policy should describe how	 IM Policy 001 – Compliance. IM Policy 023 – Privacy Impact Assessments. IM Policy 024 – Privacy Impact assessments for Disclosure for 	A1, P1A1, P54A1, P58		

General Privacy Policies/Procedures				
Topic	Description	Mitigation Strategies	Reference	
	you secure your workspaces, computers, fax machines, copiers, and other office equipment. Pay special attention to securing mobile equipment, such as notebook computers and mobile data storage devices.	 Health System Purposes. IM Policy 025 – Privacy Impact Assessments for Data Matching. IM Policy 026 – Privacy Impact Assessments for Data Matching for Research Purposes. ISP Policy Directive 4.0 – Physical and Environmental Security. AHW Information Security Handbook. 	 A1, P60 A1, P64 A5, P23 A7 	
Network & Communications Security	Measures you take to secure your network and communications infrastructure. This could include such controls as malware (anti-virus) protection, firewalls, intrusion detection systems and encryption.	 ISP Policy Directive 5.0 – Communications and Operations Management. ISP Policy Directive 7.0 – Systems Development and Maintenance. 	A5, P27A5, P54	
Access Controls	Identifying and verifying users of your health information, deciding what information they need to use, and making changes when users change positions or leave. Identification and verification includes assigning usernames, passwords and tokens.	 IM Policy 001 – Compliance. IM Policy 027 – Access to Data Holdings Process. ISP Policy directive 6.0 – Authentication and Access Control. AHW Guidance Notes for Access to Data Holdings (A2DH). AHW Information Security Handbook. 	 A1, P1 A1, P67 A5, P42 A6 A7 	
Monitoring & Audit	How you ensure that users of health information comply with your policies.	 IM Policy 001 – Compliance. IM Policy 028 – Privacy Breaches. ISP Policy Directive 1.0 – Organizational Security. ISP Policy Directive 3.0 – Personnel Security. ISP Policy Directive 5.0 – Communications and Operations Management. ISP Policy Directive 8.0 – Legislative Compliance. Provincial Logging and Audit Standard 	 A1, P1 A1, P69 A5, P7 A5, P18 A5, P27 A5, P63 A21 	
Incident Response	The plan to deal with contraventions of the HIA or your own privacy policies.	 IM Policy 001 – Compliance. IM Policy 028 – Privacy Breaches. Provincial Reportable Incident Response Process (Guide) AHW Information Security Handbook. 	• A1, P1 • A1, P69 • A9 • A7	
Business Continuity	How you ensure health information is available when needed. This includes your plans to back-up data and your plans for disaster recovery, based on business need.	 ISP Policy Directive 5.0 – Communications and Operations Management. ISP Policy Directive 7.0 – Systems Development and Maintenance. 	A5, P27A5, P54	
Change Control	Ensuring that changes to systems do not adversely affect the confidentiality, integrity or availability of health information.	ISP Policy Directive 7.0 – Systems Development and Maintenance.	■ A5, P54	

Alberta Health and Wellness Information Management Policies

Table of Contents

Compliance	2
Delegation of Oversight	4
Duty to Assist Individual's Right of Access to Information	8
Collection of Health Information	10
Collection of Personal Health Number (PHN)	12
Collection Notice	14
Use of Health Information	16
Consent-based Disclosure	18
Exceptions to Consent Based Disclosure	20
Disclosure of Information Process	22
Third Party Disclosure	24
Disclosure Notification	26
Disclosure to Police Services	31
Disclosures to Prevent Fraud or Abuse of Health Services	33
Disclosure to Prevent or Limit Fraud or Abuse of Health Services by Health Services	
Providers	35
Disclosure to protect public health and safety	37
Contracting	39
Research	41
Information Manager Agreements	43
Provincial Courier	45
Responding to requests to mask or remove information in Alberta Netcare	47
Privacy Impact Assessments	49
Privacy Impact Assessments for Disclosure for Health System Purposes	52
Privacy Impact Assessments for Data Matching	54
Privacy Impact Assessments for Data Matching for Research Purposes	56
Access to Data Holdings Process	58
Privacy Breaches	60

Compliance

Policy Statement

Alberta Health and Wellness (AHW) as custodian and all AHW affiliates must comply with the *Health Information Act* (HIA), the regulations, and the policies and procedures established or adopted under section 63(1) of the HIA.

As a public body, AHW must also comply with the *Freedom of Information and Protection of Privacy Act* (FOIP) and its regulations.

Purpose

AHW is both a custodian under the HIA and a public body under FOIP. All AHW affiliates must take steps to ensure that the HIA, the regulations, and the policies and procedures established or adopted under the HIA are complied with.

Under section 62(4) of the HIA, every affiliate of AHW must comply with:

- (a) the HIA and the regulations, and
- (b) the policies and procedures established or adopted under section 63 of the HIA.

All AHW employees must comply with the provisions of the FOIP Act, which has the following basic objectives:

- ensure that public bodies are open and accountable to the public by providing right of access to records; and
- protect the privacy of individuals by controlling the manner in which public bodies collection, retain, use, keep accurate, protect, disclose and dispose of personal information.

Applicable Groups and Assets

- AHW as custodian and as a public body
- All AHW affiliates (may include but not necessarily be limited to):
 - AHW employees
 - Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - o Students
 - o Information managers
- Subject to exceptions set out in HIA and FOIP, all information in the custody or under the control of AHW
- All AHW employees as defined under FOIP

Compliance 2

Compliance with Policy Statement

- Take the following mandatory training sessions and refresh whenever appropriate:
 - o HIA General Awareness Training
 - o FOIP General Awareness Training
 - Managing Information @ Work Training
 - Security Policy Awareness Training
- Read, stay updated about and know where to find all IM Policies (copies are available on the intranet). Refer to the linked documents section below for a list of useful resources.
- Contact the HIA helpdesk at 780-427-8089 or by email at hiahelpdesk@gov.ab.ca if you have any questions or if you are unsure if you or your business area is being compliant with the HIA, the regulations, and the policies and procedures established or adopted under section 63 of the HIA.
- Contact the FOIP Office (780-422-5111) if you have any questions regarding the FOIP Act.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA or FOIP. Failure to comply with this policy may result in:

- public investigations and Orders by the Office of the Information and Privacy Commissioner,
- fines under the HIA and FOIP,
- disciplinary action for AHW affiliates.

<u>Alignment</u>

This policy aligns with sections 62 and 63 of the HIA. This policy also aligns with the FOIP Act.

Linked Documents	Owner	Location
HIA Guidelines and Practices Manual	ICAU Unit	21 st floor, TPNT and
THA duidennes and Fractices Mandai	ICAO OTIIT	AHW Public Website
ША	AHW	Alberta Queen's Printer and
HIA	Anvv	AHW Public Website
IM Policies and Procedures	ICAU Unit	21 st floor, TPNT and
in Folicies and Frocedures	ICAO OTIIL	AHW Intranet
Information Security Policy Manual	ICAU Unit	21 st floor, TPNT and
information Security Folicy Manual		AHW Intranet
Administration of FOIP and appendices	FOIP/HIA Office	19th floor, TPNT
Administration of Fore and appendices	TOIT/THA Office	
Administration of the HIA	FOIP/HIA Office	19th floor, TPNT
Additional of the file	13117111110111100	
HIA Assignment of Responsibility Table	FOIP/HIA Office	19th floor, TPNT
The Constitution of the Sportstoffice Tuble	1311/1111/1311166	

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
1.0	June 2, 2010	ICAU Unit	ICAU Unit	System Performance and
				Information Management

Compliance 3

Delegation of Oversight

Policy Statement

Alberta Health and Wellness (AHW) as custodian must identify its affiliates who are responsible for ensuring that the *Health Information Act* (HIA), the regulations and the policies and procedures established or adopted under s.63 are complied with.

As a public body, AHW must also comply with the legal requirements set out in the *Freedom of Information and Protection of Privacy Act* (FOIP) and its regulations.

Purpose

This policy provides direction to AHW affiliates regarding established roles and the delegation of responsibility for the department under the HIA.

This policy also provides direction as to the delegation of authority under the FOIP Act.

Applicable Groups and Assets

- AHW as custodian and as a public body
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - o Students
 - o Information managers
- Subject to exceptions set out in HIA and FOIP, all information in the custody or under the control of AHW
- All AHW employees as defined under FOIP

Compliance with Policy Statement

HIA

- The senior manager of the Information Compliance and Access Unit (ICAU) Unit is the affiliate responsible for ensuring that the Parts 1, 3, 4, 5, 8 and 9 of the HIA, the regulations and the policies and procedures established or adopted under section63 are complied with.
- The senior manager of the ICAU Unit is the responsible affiliate for Part 6 of the HIA except for section 67, "power to charge fees". The FOIP/HIA coordinator and the HR/FOIP executive director are the responsible affiliates for this section as it relates to an individual's right to access information (Part 2 of the HIA).
- The senior manger of the ICAU Unit is also the responsible affiliate for Part 7 of HIA, in that he/she may be required to ensure compliance with requests and orders issued by the Commissioner.
- Contact the HIA helpdesk at 780-427-8089 or by email at hiahelpdesk@gov.ab.ca if you have any questions pertaining to designated authority under HIA.

Oversight 4

FOIP

• The FOIP/HIA Coordinator has been assigned certain responsibilities under the FOIP Act. Contact the FOIP/HIA Office (780-422-5111) with questions related to the FOIP Act or refer to the FOIP "Delegation and Assignment of Responsibility Table" in the linked documents (see below).

• Contact the FOIP/HIA Office at 780-422-5111 if you have any questions pertaining to designated authority under FOIP.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA or FOIP. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA and FOIP,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with sections 62 and 63 of the HIA. This policy also aligns with section 85(1) of the FOIP Act.

Linked documents	Owner	Location
HIA Guidelines and Practices Manual	ICAU Unit	21 st floor, TPNT and
HIA Guidennes and Practices Mandal	ICAO OTIIL	AHW Public Website
ША	AHW	Alberta Queen's Printer and
HIA	AHVV	AHW Public Website
FOIP	Government of Alberta	Alberta Queen's Printer and
TOIF	Government of Alberta	AHW Public Website
Administration of FOIP and appendices	FOIP/HIA Office	19 th floor, TPNT
Transmission of Four and appendices	,	
Administration of HIA	FOIP/HIA Office	19 th floor, TPNT
Transmission of the		
HIA Assignment of Responsibility Table	FOIP/HIA Office	19 th floor, TPNT
The Control of Responsibility Tubic	1 311 / 1111 (311166	

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
1.0	June 2, 2010	ICAU Unit	ICAU Unit	System Performance and
				Information Management

Oversight 5

Duty to Collect, Use and Disclose Health Information with the **Highest Degree of Anonymity** Possible and in a Limited Manner

Policy Statement

As a custodian under the *Heath Information Act* (HIA), Alberta Health and Wellness (AHW) and all AHW affiliates have a duty to consider the principles of "highest degree of anonymity," "least amount of information" and "need to know" when collecting, using or disclosing health information.

Purpose

The duties of custodians (and affiliates) are set out in Part 6 of the HIA and encompass a set of fair practices for health information. Under the HIA, the collection, use and disclosure of health information must, in all cases, be carried out in the most limited manner and with the highest degree of anonymity that is possible in the circumstances. The "need to know" principle is expressed in sections 24, 28 and 43 of the HIA, and under these sections AHW affiliates must collect, use and disclose health information in accordance with the affiliates' duties to the custodian.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - o Contractors/vendors
 - o Agents
 - Appointees
 - o Volunteers
 - Students
 - o Information managers
- Subject to exceptions set out in HIA, all health information in the custody or under the control of AHW (Note: The principle of the highest degree of anonymity does not apply where the collection, use or disclosure is for the purpose of providing health services or determining or verifying the eligibility of an individual to receive a health service.)

Compliance with Policy Statement

- Consider whether the collection, use and disclosure of aggregate health information is adequate for the intended purpose and if so, then use only aggregate health information.
- If aggregate health information is not adequate for the intended purpose, then consider whether other non-identifying health information is adequate for the intended purpose and if so, then use other non-identifying health information.
- If aggregate and other non-identifying health information is inadequate for the intended purpose, individually identifying health information may be collected, used or disclosed if the collection, use or disclosure is authorized by the HIA and is carried out in accordance with the HIA.
- Collect, use or disclose only the least amount of health information necessary to achieve the intended purpose.
- Collect, use or disclose health information only in a manner that is in accordance with that affiliate's duties to the custodian.

• Contact the HIA help desk (427-8087 or hiahelpdesk@gov.ab.ca) if you have questions about collecting, using or disclosing the least amount of information, using the highest degree of anonymity and based on a need to know.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

<u>Alignment</u>

This policy statement aligns with sections 24, 28, 43, 57 and 58 of the HIA.

Linked documents	Owner	Location
Chapters 5-8 of the HIA Guidelines and Practices Manual	Information Compliance and Access Unit (ICAU)	21 st Floor, TPNT and AHW Public Website

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
2.0	June 2, 2010	ICAU Unit	ICAU Unit	System Performance and
				Information Management
1.0	luno 12, 2002	RAPS Unit	Linda Miller, Director,	Todd Heron, ADM, Health
1.0	June 13, 2003	KAPS UTIL	IM Branch	Accountability Division

Duty to Assist Individual's Right of Access to Information

Policy Statement

On request, Alberta Health and Wellness (AHW) as custodian and as a public body (including all AHW affiliates and employees) must make every reasonable effort to assist an applicant who makes a request to access a record that is in the custody or under the control of AHW. AHW must respond to each applicant openly, accurately and completely.

Purpose

An individual has a right of access to any record containing health information about the individual that is in the custody or under the control of AHW under section 7(1) of the *Health Information Act* (HIA).

An individual has a right of access to any record in the custody or under the control of a public body including a record containing personal information about the applicant under section 6(1) of the Freedom of Information and Protection of Privacy Act (FOIP).

Applicable Groups and Assets

- AHW as custodian and as a public body
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - Students
 - o Information managers
- Subject to exceptions set out in HIA and FOIP, all information in the custody or under the control of AHW
- All AHW employees as defined under FOIP

Compliance with Policy Statement

- All requests to access information under the HIA and FOIP should be forwarded as soon as possible to the FOIP/HIA Office (780-422-5111).
- All requests to correct or amend information under the HIA and FOIP should be forwarded as soon as possible to the FOIP/HIA Office (780-422-5111).
- If individuals are unsure how to make a formal access request under the HIA then refer them to the "HIA Request to Access Information" form on the AHW public website (linked below).
- If individuals are unsure how to make a formal access request under FOIP then refer them to the "FOIP Request to Access Information" form on the Government of Alberta website (linked below).
- If there is an existing access process such as the statement of benefits paid process, the individual may choose the existing process to access the information without the formality and administrative burden of making a request pursuant to the HIA.
- If you have any questions concerning HIA access requests, call the FOIP/HIA office general line at 780-422-5111, the HIA helpdesk at 780-427-8089 or email at hiahelpdesk@gov.ab.ca.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA or FOIP. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA and FOIP,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with sections 7 - 17 and 87 of the HIA.

This policy statement aligns with sections 6, 7(1) and 36(1) of FOIP.

Linked documents	Owner	Location
Chapters 2-4 of the HIA Guidelines and	Information Access and	21 st Floor, TPNT and AHW
<u>Practices Manual</u>	Compliance Unit (ICAU)	Public Website
HIA Request to Access Information Form	ICA Unit	21 st Floor, TPNT and AHW
HIA Request to Access Information Form	ICA OIIII	Intranet
FOIP Request to Access Information	Government of Alberta	GoA Public Website
<u>Form</u>	Government of Alberta	GOTT UBITE WEBSITE
HIA Internal Policy and Procedures	FOIP/HIA Office	19 th Floor, TPNT and AHW
THA Internal Folicy and Procedures	TOIF/THA Office	Public Website
HIA Delegation Of Authority Matrix (Part	FOIP/HIA Office	19 th Floor, TPNT
<u>2)</u>	FOIF/HIA Office	15 FIOUI, IFINI

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
2.0	June 2, 2010	ICAU Unit	ICA Unit	System Performance and
				Information Management
1.0	luna 12, 2002	DADC Linit	Linda Miller Director IM	Todd Heron ADM Health
1.0	1.0 June 13, 2003 RAPS Un	RAPS Unit	Branch	Accountability Division

Collection of Health Information

Policy Statement

As a custodian, Alberta Health and Wellness (AHW) and its affiliates must only collect health information in accordance with the *Health Information Act* (HIA).

<u>Purpose</u>

To help ensure that AHW as custodian and its affiliates only collect health information in accordance with HIA.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - Volunteers
 - Students
 - o Information managers
- Subject to exceptions set out in the HIA and FOIP, all health information collected by AHW and its
 affiliates

Compliance with Policy Statement

- Non-identifying health information may be collected for any purpose.
- AHW may collect individually identifying health information for a series of specific purposes (under section 27 (1) and (2) of HIA). The most common reasons include:
 - o for the purpose of providing a health service;
 - o determining or verifying eligibility to receive a health service;
 - o if the collection is authorized by an enactment of Alberta or Canada;
 - o health system management.
- Collect health information in a limited manner, collecting only the amount of information that is essential to carry out the intended purpose.
- Collect health information directly from the individual unless indirect collection is authorized by the HIA.
- Contact the HIA help desk in the Information Compliance and Access Unit (ICAU), AHW, if you have any questions (780 427-8089 or hiahelpdesk@gov.ab.ca).

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

<u>Alignment</u>

This policy statement aligns with section 18 of the HIA.

Linked documents	Owner	Location
Chapter 6 of the HIA Guidelines and	ICAU	21 st floor, TPNT
<u>Practices Manual</u>	ICAU	AHW Public Website

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health System
1.0	June 2, 2010	ICAU Unit	ICAU	Performance and Information
				Management

Collection of Personal Health Number (PHN)

Policy Statement

Alberta Health and Wellness (AHW) as custodian has the right to require an individual to provide the individual's PHN based on a need to know that information.

Purpose

The PHN provides a single point of access to an individual's identifying health information and is therefore a critical point of risk. As such, the *Health Information Act* (HIA) intentionally limits the collection of PHNs. Only custodians or persons designated by the *Health Information Regulation* can require an individual to provide his/her PHN under section 21(1).

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - Students
 - o Information managers
- An individual's PHN

Compliance with Policy Statement

- When requesting a PHN from an individual, AHW must advise the individual of its authority to collect that PHN.
- If you are unsure whether you should be collecting PHNs or have questions about AHW's authority to collect PHNs, then contact the HIA help desk in the Information Compliance and Access Unit (ICAU), AHW, at 780-427-8089 or hiahelpdesk@gov.ab.ca.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with section 21 of the HIA.

Linked documents	Owner	Location
Chapter 6 of the HIA Guidelines and	ICAU	21 st floor, TPNT
Practices Manual	ICAU	AHW Public Website

Version	Date	Author	Reviewers	Approval
1.0	June 2, 2010	ICAU	ICAU	Mark Brisson, A/ADM, Health System
1.0	Julie 2, 2010	ICAU	10/10	Performance and Information Management

Collection Notice

Policy Statement

When collecting individually identifying health information about an individual directly from the individual, Alberta Health and Wellness (AHW) as custodian and its affiliates must provide the individual with a collection notice.

Purpose

Section 22(3) of the *Health Information Act* (HIA) states that when collecting individually identifying health information about an individual directly from the individual, the custodian must take reasonable steps to inform the individual (a) of the purpose for which the information is collected, (b) of the specific legal authority for the collection, and (c) of the title, business address and business telephone number of an affiliate of the custodian who can answer the individual's questions about the collection.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - o Students
 - Information managers
- Individually identifying health information collected directly from the individual who is the subject
 of that information.

Compliance with Policy Statement

- A collection notice may take several forms including:
 - providing oral notification to individuals
 - o printing it on a collection form
 - providing the notice in an accompanying publication such as a brochure about a service
 - providing the notice via a poster on the wall or service counter
 - o providing an option on an interactive voice response system
 - o providing a pop up screen as part of a computer program
- The notice must contain all three elements in section 22(3) of the HIA, as listed in the purpose section above.
- Some form of notice should be given to the individual before the information is collected so that the individual has an opportunity to make an informed decision as to whether to provide the information as well as be aware of the consequences that may result from not doing so. An explanatory document may be provided at a later time.

Collection Notice 14

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

<u>Alignment</u>

This policy statement aligns with section 22(3) of the HIA.

Linked documents	Owner	Location
Chapter 6 of the HIA Guidelines and	Information Compliance	21 st floor, TPNT and
<u>Practices Manual</u>	and Access Unit (ICAU)	AHW Public Website
Collection Natice Cuidelines	ICALL	21 st floor, TPNT and AHW
Collection Notice Guidelines	ICAU	Intranet

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
2.0	June 2, 2010	ICAU	ICAU	System Performance and
				Information Management
1.0	luna 12, 2002	DADC Linit	Linda Miller, Director IM	Todd Heron, ADM Health
1.0	June 13, 2003	RAPS Unit	Branch	Accountability Division

Collection Notice 15

Use of Health Information

Policy Statement

Alberta Health and Wellness (AHW) as custodian and its affiliates shall only use health information in its custody or under its control in compliance with the *Health Information Act* (HIA).

Purpose

To ensure that AHW as custodian and its affiliates understand how to appropriately use health information as set out in the HIA. This includes understanding the appropriate and controlled access to and sharing of health information within the department listed in section 27(1) of the HIA as well as the additional uses of health information that involve sharing that information beyond the department (section 27(2)).

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - o Students
 - Information managers
- Subject to the exceptions set out in HIA, all health information in the custody or under the control
 of AHW.

<u>Compliance with Policy Statement</u>

- Use only the least amount of individually identifying health information with the highest degree of anonymity, based on a need to know.
- AHW as custodian and its affiliates may use non-identifying health information for any purpose under section 26 of the HIA.
- AHW as custodian and its affiliates may use individually identifying health information in its custody or under its control for any of the purposes listed in section 27
- To assist with using health information, refer to the "Use of Health Information Decision Tree" and the "Considerations for Use" guideline document located under the linked documents.
- Because the department has additional health system mandates, the department has additional authorized uses of health information under section 27(2) of the HIA:
 - Planning and resource allocation
 - Health system management
 - o Public health surveillance
 - Health policy development

Use of Health Information 16

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with sections 25-30, 57 and 58 of the HIA.

Linked documents	Owner	Location
Use of Health Information Decision Tree	Information Compliance	21 st Floor, TPNT and AHW
Ose of Health Information Decision free	and Access Unit (ICAU)	Intranet
Chapter 7 of the HIA Guidelines and	ICAU	21 st Floor, TPNT
Practices Manual	ICAU	and AHW Public Website
Considerations for Use	ICALL	21 st floor, TPNT and AHW
Considerations for Use	ICAU	Intranet

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
2.0	June 2, 2010	ICAU	ICAU	System Performance and
				Information Management
1.0	luna 12, 2002	DADC Heit	Linda Miller Director IM	Todd Heron ADM Health
1.0	June 13, 2003	RAPS Unit	Branch	Accountability Division

Consent-based Disclosure

Policy Statement

Subject to the exceptions noted in the *Health Information Act* (HIA), Alberta Health and Wellness (AHW) as custodian and its affiliates may disclose individually identifying health information to a person other than the individual who is the subject of the information if the individual or the individual's authorized representative has consented to the disclosure.

Purpose

Individually identifying health information may be disclosed to a person other than the individual who is the subject of the information if the individual or the individual's representative has consented to that disclosure.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - o Students
 - Information managers
- Subject to the exceptions set out in the HIA, all individually identifying health information in the custody or under the control of AHW

Compliance with Policy Statement

- Consent should only be sought when required.
- Consent should never be implied. Consent should be informed and voluntary.
- Consent may either be obtained directly from the individual who is the source of that information or from a person who is acting on behalf of that individual under section 104(1)(c) to (i).
- Consent under section 34 must be provided in writing or electronically and must include the following:
 - o an authorization for the custodian to disclose the health information specified in the consent
 - o the purpose for which the health information may be disclosed
 - o the identity of the person to whom the health information may be disclosed
 - an acknowledgement that the individual providing the consent has been made aware of the reasons why the health information is needed and the risks and benefits to the individual of consenting or refusing to consent
 - o the date the consent is effective and the date, if any, on which the consent expires (AHW should try and avoid promoting a blanket consent)
 - a statement that the consent may be revoked at any time by the individual providing it
- The section 34 consent form located under the linked documents section follows the requirements above and may be used as a template for requesting consent. If your program area would like to amend this consent form to meet the specific needs of your program area, please consult with the

Information Compliance and Access (ICAU) Unit before amending the forms. ICAU may be contacted at 780-427-8089 or via email at hiahelpdesk@gov.ab.ca.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

<u>Alignment</u>

This policy statement aligns with section 34 and 104(1)(c) to (i) of the HIA and section 6 of the Health Information Regulation.

Linked documents	Owner	Location	
Section 34 Consent Form	ICAU	AHW Public Website	
Chapter 8 of the HIA Guidelines and	ICALL	21 st Floor, TPNT and	
<u>Practices Manual</u>	ICAU	AHW Public Website	

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
2.0	June 2, 2010	ICAU	ICAU	System Performance and
				Information Management
1.0	lung 12, 2002	RAPS	Linda Miller, Director	Todd Heron ADM Health
1.0	June 13, 2003	Unit	IM Branch	Accountability Division

Exceptions to Consent Based Disclosure

Policy Statement

Alberta Health and Wellness (AHW) as custodian and its affiliates may disclose individually identifying diagnostic, treatment and care information without the consent of the individual who is the subject of the information for any of the specific circumstances identified in section 35(1) and (4) of *Health Information Act* (HIA).

Purpose

Section 35 of the HIA provides for limited and specific exceptions to the disclosure of health information without consent. Disclosures pursuant to sections 35(1) and (4) require the maintenance of certain disclosure information (section 41) and recipients of individually identifying diagnostic, treatment and care information must be notified of the purpose and authority for the disclosure (section 42).

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - Contractors/vendors
 - o Agents
 - Appointees
 - o Volunteers
 - o Students
 - Information managers
- Subject to exceptions set out in the HIA, all individually identifying diagnostic, treatment and care information in the custody or under the control of AHW

Compliance with Policy Statement

- Consult with the "Exceptions to Consent Based Disclosure" list in the linked documents and/or section 35 of HIA to ensure that the disclosure fits with exceptions to consent based disclosure.
- See the Disclosure Notice policy for rules regarding notification when disclosing diagnostic, treatment and care information.
- If you have any questions regarding disclosure of health information, please contact the HIA helpdesk (780-427-8089 or hiahelpdesk@gov.ab.ca).

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with sections 35, 41 and 42 of the HIA.

Linked documents	Owner	Location
Exceptions to Consent Based Disclosure	Information Compliance	21 st Floor, TPNT and
List	and Access Unit (ICAU)	AHW Intranet Site
Chapter 8 of the HIA Guidelines and	ICALL	21 st Floor, TPNT and
Practices Manual	ICAU	AHW Public Website

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
2.0	June 2, 1010	ICAU	ICAU	System Performance and
				Information Management
1.0	luna 12, 2002	DADC Linit	Linda Miller, Director IM	Todd Heron ADM Health
1.0	June 13, 2003	RAPS Unit	Branch	Accountability Division

Disclosure of Information Process

Policy Statement

The Information Compliance and Access Unit (ICAU) will provide advice on the disclosure of individually and/or potentially identifiable health information for Alberta Health and Wellness (AHW).

Purpose

This policy helps to ensure that all disclosures of individually and/or potentially identifiable health information comply with the *Health Information Act* (HIA) and other relevant legislation.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - Students
 - Information managers
- Subject to exceptions set out in HIA, all health information in the custody or under the control of AHW

Compliance with Policy

AHW affiliates must consult with ICAU (780-427-8089) about disclosures of individual and/or
potentially identifiable health information subject to the following exceptions; all disclosures to
individuals that the information is about (i.e., HIA access requests, statement of benefits paid,
AHCIP/Premiums issues); consented disclosures to third parties; all routine and/or publicly
available data products or other summarized aggregate data products; and direct/live access to
electronic data sources held by the department. (Use of health information by AHW affiliates is
governed by the access to data holding policy).

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with the HIA.

Linked documents	Owner	Location
Chapter 8 of the HIA Guidelines and	ICAU	21 st Floor, TPNT and
<u>Practices Manual</u>	ICAU	AHW Public Website
Data Disclosure Guidelines	Information and Analysis	

Version	Date	Author	Reviewers	Approval
	June 2, 2010	ICAU	ICAU	Mark Brisson, A/ADM, Health
2.0				System Performance and
				Information Management
1.0	June 13, 2003	RAPS	Linda Miller Director IM	Todd Heron ADM Health
		Unit	Branch	Accountability Division

Third Party Disclosure

Policy Statement

When Alberta Health and Wellness (AHW) as custodian and its affiliates are dealing with requests from third parties to disclose individually identifying health information about a specific individual, there must be a legislative authority for the disclosure.

Purpose

When dealing with third parties, such as lawyers, insurance companies, Workers Compensation Board, etc. it is important for AHW affiliates to give consideration to the authority for these disclosures and not simply assume that the third party has authority.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - Students
 - Information managers
- Subject to exceptions set out in HIA, all individually identifying health information in the custody or under the control of AHW

Compliance with Policy Statement

- Disclose health information in accordance with the rules governing disclosure set out in sections 31 to 56 of the *Health Information Act* (HIA).
- Apply the principles of highest degree of anonymity, least amount of information and need to know before disclosing any health information.
- Consider as a factor, together with any other relevant factors, any expressed wishes of the individual who is the subject of the information before deciding how much, if any, information should be disclosed (section 58(2)).
- Contact the HIA helpdesk (780-427-8089 or highertright highertright
 LLS will be consulted by the helpdesk [part of the Information Compliance and Access Unit (ICAU)] as required.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

<u>Alignment</u>

This policy statement aligns with sections 31-58 of the HIA.

Linked documents	Owner	Location
Chapters 3 and 8 of the HIA Guidelines and Practices Manual	ICAU	21 st Floor, TPNT and AHW Public Website
Section 34(2) Consent Form	ICAU	21 st Floor, TPNT and AHW Public Website

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
2.0	June 2, 2010	ICAU	ICAU	System Performance and
				Information Management
1.0	luna 12, 2002	DADC	Linda Miller Director	Todd Heron ADM Health
1.0	June 13, 2003	RAPS	IM Branch	Accountability Division

Disclosure Notification

Policy Statement

When disclosing individually identifying diagnostic, treatment and care information, Alberta Health and Wellness (AHW) as custodian and its affiliates must provide the recipient with a disclosure notice subject to some exceptions.

Purpose

Section 42(1) of the *Health Information Act* (HIA) states that a custodian disclosing individually identifying diagnostic, treatment and care information must inform the recipient in writing of the purpose for the disclosure and the authority under which the disclosure is made.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - Contractors/vendors
 - o Agents
 - o Appointees
 - Volunteers
 - o Students
 - o Information managers
- Subject to exceptions set out in HIA, all individually identifying diagnostic, treatment and care information in the custody or under the control of AHW.

Note: This policy does not apply where the disclosure is:

- o To another custodian (section 35(1)(a) and section 47)
- o To the Minister or the Department (section 46)
- o To a police service or the Minister of Justice and Attorney General (sections 37.1 and 37.3)
- o To the individual who is the subject of the information (section 42(2)(e).

Compliance with Policy Statement

- Confirm that diagnostic, treatment and care information is the type of information being disclosed. Check with the HIA helpdesk (780-427-8089 or hiahelpdesk@gov.ab.ca) if you are unsure.
- Confirm with your business unit whether disclosure notification(s) have been or still need to be sent. Make sure that the notification(s) meets with the following requirements:
 - o The notice must be in writing
 - o The notice must inform the recipient of the purpose of the disclosure
 - The notice must inform the recipient of the authority under which the disclosure was made
- Each business area should retain a copy of disclosure notices that have been issued by that business area.
- To help ensure compliance with this policy, use the appropriate disclosure notice template form. All disclosure notice template forms are available under the linked documents section.

Disclosure Notice 26

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with section 42 of the HIA.

Linked documents	Owner	Location
	Information	21 st Floor, TPNT
Section 42 Notice with Consent Form	Compliance and	and AHW Intranet Site/GNP Manual
	Access Unit (ICAU)	and Anw intranet Site/Give Mandai
Section 42 Notice without Consent	ICAU	21 st Floor, TPNT
Form		and AHW Intranet Site/GNP Manual
Section 42 Notice Non-Identifying	ICAU	21 st Floor, TPNT
Information		and AHW Intranet Site
Chapter 8 of the HIA Guidelines and	ICAU	21 st Floor, TPNT and AHW Public
<u>Practices Manual</u>		Website

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
1.0	June 2, 2010	ICAU	ICAU	System Performance and
				Information Management

Disclosure Notice 27

SECTION 42 NOTICE TO RECIPIENT TO ACCOMPANY THE DISCLOSURE OF INDIVIDUALLY IDENTIFYING DIAGNOSTIC, TREATMENT AND CARE INFORMATION BY A CUSTODIAN

Disclosure with the Subject's Consent

The attached individually identifying diagnostic, treatment and c	care information of
	(subject of information)
is being disclosed to	(name of recipient)
by	(name of custodian) on
(date), with the consent of	(name of the
subject) under section 34 of the Health Information Act, only for t	he following purpose(s):
Name and Signature of Custodian (or affiliate)	Pate

Disclosure Notice 28

SECTION 42 NOTICE TO RECIPIENT TO ACCOMPANY THE DISCLOSURE OF INDIVIDUALLY IDENTIFYING DIAGNOSTIC, TREATMENT AND CARE INFORMATION BY A CUSTODIAN

Disclosure without the Subject's Consent:

Th	e attached individually identifying diagnostic, treatment and care information of (named individual subject) has been disclosed to
rec	(name of ipient/custodian) on (date), without the consent of the subject, but is horized under the following provision(s) of the <i>Health Information Act</i> (mark the appropriate box).
	To another custodian for any or all of the purposes listed in section 27(1) or (2) of the HIA, as the case may be.
	To the government of Canada or of another province or territory of Canada for that government's use for health system planning and management and health policy development where
	 i) the individual is a resident of that other province or territory, or ii) that government is otherwise responsible for payment for health services provided to the individual.
	To provide continuing treatment and care to the above individual (s.35(1)(b)).
	To provide information concerning the presence, location, condition, diagnosis, progress and prognosis of the above individual on the above date and the above individual has not requested otherwise (s.35(1)(c)) (Note – recipient must be a family member or another person with whom the individual is believed to have a close personal relationship).
	To advise family members of the above individual, or a person with whom the above individual is believed to have a close personal relationship, that the individual has been injured, is ill or has died and the individual has not requested otherwise (s.35(1)d)).
	To provide health services to the above individual who is being detained in a penal or other custodial facility (s.35(1)(e)).
	To conduct an audit of the information (s.35(1)(f)) (Note – recipient must enter into an agreement with the custodian about non-disclosure and destruction of the information).
	To carry out quality assurance activities within the meaning of section 9 of the Alberta Evidence Act (s.35(1)(g)).
	To provide information for a court proceeding or a proceeding before a quasi-judicial body (s.35(1)(h)) (Note – the custodian must be a party to the proceeding).

Name	e and Signature of Custodian (or affiliate) Date
	To enable the Minister of Health and Wellness to carry out his duties (s.40) (Note – the custodian must determine if the disclosure is necessary or desirable)
	To allow for permanent preservation and historical research by the Provincial Archives of Alberta or another archives that is subject to this Act or the Freedom of Information and Protection of Privacy Act (s.38) (Note—the custodian must determine that the information has enduring value).
	To enable a health professional body to conduct an investigation, a discipline proceeding, a practice review or an inspection (s.35(4)) (Note – the custodian must comply with other relevant legislation and the health professional body must enter into an agreement with the custodian about nondisclosure and destruction of the information).
	To transfer records to a successor custodian because the first custodian is ceasing to be a custodian $(s.35(1)(q))$.
	To comply with another act or regulation of Alberta or Canada that authorizes or requires the disclosure (s.35(1)(p)).
	To provide necessary health services to a descendant of a deceased individual (s.35(1)(o)) (Note – the recipient must be a descendant or a representative under section 104(1)(c) to (i) and the privacy of the deceased individual must be protected).
	To act in the best interests of the above individual if the individual lacks the mental capacity to provide consent $(s.35(1)(n))$.
	To avert or minimize an imminent danger to the health or safety of any person (s.35(1)(m)).
	To enable an officer of the Legislature (e.g. Auditor General, Ombudsman, Chief Electoral Officer, Information and Privacy Commissioner) to carry out his/her duties (s.35(1)(l)).
	To detect or prevent fraud, limit abuse in the use of health services or prevent the commission of an offence under an enactment of Alberta or Canada (s.35(1)(k)) (Note – the recipient must be another custodian).
	To investigate an offence involving a life-threatening personal injury to the above individual and the above individual has not requested otherwise (s.35(1)(j)) (Note – the recipient must be a municipal or provincial police service).
	To comply with a subpoena, warrant or court order compelling the production of information or with a rule of court that relates to the production of information (s.35(1)(i)) (Note – the recipient body must have jurisdiction to compel the production of information).

Disclosure to Police Services

Policy Statement

Alberta Health and Wellness (AHW) as custodian may disclose limited individually identifying health information without consent to a police service where the disclosure is permitted under section 35(1) of the *Health Information Act* (HIA).

Purpose

Police services may make requests for health information from AHW. When considering whether to disclose individually identifying health information in response to these requests, AHW must ensure that the legal requirements of the HIA are met. Police disclosures may occur under section 35(1) of the HIA in the following ways:

- where an individual is injured, ill or deceased, so that family members of the individual or another
 person with whom the individual is believed to have a close personal relationship or a friend of the
 individual can be contacted, if the disclosure is not contrary to the express request of the individual
 35(1)(d)
- to an official of a penal or other custodial institution in which the individual is being lawfully detained if the purpose of the disclosure is to allow the provision of health services or continuing treatment and care to the individual 35(1)(e)
- for the purpose of complying with a subpoena, warrant or order issued or made by a court, person or body having jurisdiction in Alberta to compel the production of information or with a rule of court binding in Alberta that relates to the production of information 35(1)(i)
- if AHW believes, on reasonable grounds, that the disclosure will avert or minimize imminent danger to the health or safety of any person 35(1)(m)
- if that individual lacks the mental capacity to provide a consent and, in the opinion of the custodian, disclosure is in the best interest of the individual 35(1)(n)
- if the disclosure is authorized or required by an enactment of Alberta or Canada 35(1)(p)

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - Volunteers
 - Students
 - Information managers
 - Subject to exceptions set out in HIA, all individually identifying health information

Compliance with Policy Statement

- All requests for disclosure of health information made by a police service are to be forwarded to the HIA help desk (780-427-8089 or hiahelpdesk@gov.ab.ca).
- The HIA help desk will forward the request to the HIA policy manager in the Information Compliance and Access Unit (ICAU).
 - o The HIA policy manager will contact and consult with Legal and Legislative Services (LLS) on these disclosures.

Disclosure to Police Services 31

 The HIA policy manager may require that a written request be submitted by the police service detailing the grounds on which they believe a disclosure is necessary and authorized before any decision is made to disclose information.

- o If individually identifying health information is disclosed, then only the least amount of information should be disclosed to achieve the intended purpose.
- o Letters, forms and supporting documents will be filed in ICAU.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with section 35(1) of the HIA.

Linked documents	Owner	Location
Chapter 8 of the HIA Guidelines and Practices Manual	ICAU	21 st Floor, TPNT and AHW Intranet Site
OIPC Police Disclosure Guidelines	Office of the Information and Privacy Commissioner	9925 109 Street and www.oipc.ab.ca

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
1.0	June 2, 2010	ICAU	ICAU	System Performance and
				Information Management

Disclosure to Police Services 32

Disclosures to Prevent Fraud or Abuse of Health Services

Policy Statement

Alberta Health and Wellness (AHW) as custodian may disclose limited individually identifying health information without consent to a police service or the Minister of Justice and Attorney General where it reasonably believes that the information relates to a possible commission of an offence and that the disclosure will detect or prevent fraud or limit abuse in the use of health services.

Purpose

Disclosures to prevent fraud or abuse of health services may be considered in response to:

- an external request, for example, a request made by a policy service
- a request from within the department, for example, where an AHW employee has identified a situation where he/she reasonably believes that fraud may be prevented.

In either instance, the requirements for disclosure under section 37.1 of the *Health Information Act* (HIA) must be met before AHW discloses any individually identifying health information. If individually identifying health information is disclosed, then only the least amount of information selected from within the limited data set (listed below) should be disclosed to achieve the intended purpose.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - Students
 - o Information managers
- Limited data set of health information in custody or under the control of AHW pertaining to a specific investigation:
 - o The name, date of birth and personal health number (PHN) of an individual
 - o The nature of any injury or illness of an individual
 - o The date and location a health service was sought or received by an individual
 - o The name of any drug and date it was provided to or prescribed for an individual
 - Health services provider information about a health services provider from whom that individual sought or received health services if that information is appropriate for the circumstances and if AHW has already disclosed health information about the individual in question

Compliance with Policy Statement

- All requests for disclosure of health information to prevent or limit fraud or abuse of health services are to be forwarded to the HIA help desk (780-427-8089 or hiahelpdesk@gov.ab.ca).
- The HIA help desk will forward the request to the HIA policy manager in the Information Compliance and Access Unit (ICAU).
 - The HIA policy manager will contact and consult with Legal and Legislative Services (LLS) on these disclosures.

 The HIA policy may require that a written request be submitted by the police service detailing the grounds on which they believe a disclosure is necessary and authorized before any decision is made to disclose information.

- The HIA policy manager will apply the following two questions to the information provided:
 - Is the information related to the possible commission of an offence under a statute or regulation of Alberta or Canada?
 - Will the disclosure detect or prevent fraud or limit abuse in the provision of health services?
- o If the HIA policy manager reasonably believes that the answer to either question is "no", then he/she will not disclose any information and will inform the parties that made the request.
- o If the HIA policy manager reasonably believes that the answer to both questions is "yes", then the HIA policy manager may disclose the requested information and will contact the parties who have made the request.
- Letters, forms and supporting documents will be filed in the ICAU.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with section 37.1 of the HIA.

Linked documents	Owner	Location
Chapter 8 of the <u>HIA Guidelines and</u> <u>Practices Manual</u>	ICAU	21 st Floor, TPNT and AHW Intranet Site
OIPC Police Disclosure Guidelines	Office of the Information and Privacy Commissioner	9925 109 Street and www.oipc.ab.ca

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
1.0	June 2, 2010	ICAU	ICAU	System Performance and
				Information Management

IM POLICY 016 June 2, 2010

Disclosure to Prevent or Limit Fraud or Abuse of Health Services by Health Services Providers

Policy Statement

Alberta Health and Wellness (AHW) as a custodian may disclose limited individually identifying health information without consent to a police service or the Minister of Justice and Attorney General where it reasonably believes that the information relates to a possible commission of an offence and that the disclosure will detect or prevent fraud or limit abuse of health services by a health services provider.

Purpose

Disclosures to prevent fraud or abuse of health services by health services providers may be considered in response to:

- an external request, for example, a request made by a policy service
- a request from within the department, for example, where an AHW employee has identified a situation where he/she reasonably believes that fraud may be prevented.

In either instance, the requirements for disclosure under the *Alberta Health Care Insurance Act* must be met before AHW discloses any individually identifying health information. If individually identifying health information is disclosed, then only the least amount of information selected from within the limited data set (listed below) should be disclosed to achieve the intended purpose.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily limited to):
 - AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - Volunteers
 - o Students
 - o Information managers
- Limited data set of health information in custody or under the control of AHW pertaining to a specific investigation:
 - o The name and business address of health services provider
 - o The date health services provider provided a health service and description of that service
 - o The benefits paid or charged for a health service by a health services provider
 - o Individually identifying health information about the individual who received that health service of that information is related to that health service

Compliance with Policy Statement

- All requests for disclosure of health information to prevent or limit fraud or abuse of health services by health services providers should be forwarded to the Health Information Act (HIA) help desk (780-427-8089 or hiahelpdesk@gov.ab.ca).
- The HIA help desk will forward the request to the HIA policy manager in the Information Compliance and Access Unit (ICAU).
 - The HIA policy manager will contact and consult with Legal and Legislative Services (LLS) on these requests.

IM POLICY 016 June 2, 2010

 The HIA policy may require that a written request be submitted by the police service detailing the grounds on which they believe a disclosure is necessary and authorized before any decision is made to disclose information.

- The HIA policy manager will apply the following two questions to the information provided on the form:
 - Is the information related to the possible commission of an offence under a statute or regulation of Alberta or Canada?
 - Will the disclosure detect or prevent fraud or limit abuse in the provision of health services?
- o If the HIA policy manager reasonably believes that the answer to either question is "no", then he/she will not disclose any information and will inform the parties that made the request.
- If the HIA policy manager reasonably believes that the answer to both questions is "yes", then
 the HIA policy manager may disclose the requested information and will contact the parties
 who have made the request.
- o Letters, forms and supporting documents will be filed in the ICAU Unit.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- public investigations and Orders by the Office of the Information and Privacy Commissioner,
- fines under the HIA,
- disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with the Alberta Health Care Insurance Act.

Linked documents	Owner	Location
Chapter 8 of the <u>HIA Guidelines and</u> <u>Practices Manual</u>	ICAU	21 st Floor, TPNT and AHW Intranet Site
OIPC Police Disclosure Guidelines	Office of the Information and Privacy Commissioner	9925 109 Street and www.oipc.ab.ca

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
1.0	June 2, 2010	ICAU	ICAU	System Performance and
				Information Management

IM POLICY 017 June 2, 2010

Disclosure to protect public health and safety

Policy Statement

Alberta Health and Wellness (AHW) as a custodian may disclose limited individually identifying health information without consent to a police service or the Minister of Justice and Attorney General where it reasonably believes that the information relates to a possible commission of an offence and that the disclosure will protect the health and safety of Albertans.

Purpose

Disclosures to protect public health and safety may be considered in response to:

- an external request, for example, a request made by a policy service
- a request from within the department, for example, where an AHW employee has identified a situation where he/she reasonably believes that fraud may be prevented.

In either instance, the requirements for disclosure under section 37.3 of the *Health Information Act* (HIA) must be met before AHW discloses any individually identifying health information. If individually identifying health information is disclosed, then only the least amount of information selected from within the limited data set (listed below) should be disclosed to achieve the intended purpose.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - Students
 - o Information managers
- Limited data set of health information in custody or under the control of AHW pertaining to a specific investigation:
 - o The name and date of birth of an individual
 - The nature of illness or injury
 - o The data and location that health service was sought or received
 - o Whether sample of bodily substance was taken
 - o Information specified in section 1(1)(i)(ii) about a health services provider who provided a health service to an individual referred to in subsection (1).

Compliance with Policy Statement

- All requests for disclosure of health information to protect public health and safety should be forwarded to the HIA help desk (780-427-8089 or hiahelpdesk@gov.ab.ca).
- The HIA help desk will forward the request to the HIA policy manager in the Information Compliance and Access Unit (ICAU).
 - The HIA policy manager will contact and consult with Legal and Legislative Services (LLS) on these requests.

IM POLICY 017 June 2, 2010

 The HIA policy may require that a written request be submitted by the police service detailing the grounds on which they believe a disclosure is necessary and authorized before any decision is made to disclose information.

- The HIA policy manager will apply the following two questions to the information provided:
 - Is the information related to the possible commission of an offence under a statute or regulation of Alberta or Canada?
 - Will the disclosure protect the health and safety of Albertans?
- o If the HIA policy manager reasonably believes that the answer to either question is "no", then he/she will not disclose any information and will inform the parties that made the request.
- If the HIA policy manager reasonably believes that the answer to both questions is "yes", then
 the HIA policy manager may disclose the requested information and will contact the parties
 who have made the request.
- o Letters, forms and supporting documents will be filed in the ICAU.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- public investigations and Orders by the Office of the Information and Privacy Commissioner,
- fines under the HIA,
- disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with section 37.3 of the HIA.

Linked documents	Owner	Location
Chapter 8 of the HIA Guidelines and Practices Manual	ICAU	21 st Floor, TPNT and AHW Intranet Site
OIPC Police Disclosure Guidelines	Office of the Information and Privacy Commissioner	9925 109 Street and www.oipc.ab.ca

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
1.0	June 2, 2010	ICAU	ICAU	System Performance and
				Information Management

IM POLICY 018 June 2, 2010

Contracting

Policy Statement

Alberta Health and Wellness (AHW) must ensure that all of its contractors comply with the *Health Information Act* (HIA) and the *Freedom of Information and Protection of Privacy* (FOIP) Act.

Purpose

Section 62(4) of the HIA states that each affiliate of a custodian must comply with (a) this Act and the regulations, and (b) the policies and procedures established or adopted under section 63. Contractors and vendors for AHW are considered affiliates under the HIA.

Contractors must comply with FOIP.

Applicable Groups and Assets

- AHW as custodian and as a public body
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - Contractors/vendors
- All information in the custody or under the control of AHW

Compliance with Policy Statement

- Consult with Legal and Legislative Services when developing contracts so that they may ensure compliance with the HIA and FOIP.
- All successful contractors and vendors must attend the mandatory HIA general awareness training session. Contact the HIA help desk (780-427-8089 or hiahelpdesk@gov.ab.ca) in the Information Access and Compliance Unit (ICAU) to sign up.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA or FOIP. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA and FOIP,
- o disciplinary action for AHW affiliates.

<u>Alignment</u>

This policy statement aligns with the sections 62(4) of HIA.

Contracting 39

IM POLICY 018 June 2, 2010

Linked documents	Owner	Location
Chapters 5, 7, 8, 9, and 11 of the HIA Guidelines and Practices Manual	ICAU	21 st Floor, TPNT and AHW Public Website
Public-sector Outsourcing & Risks to Privacy	OIPC	410, 9925 - 109 Street and OIPC Website
OIPC Investigation Reports <u>H2002-001</u> & <u>H2001-IR-009</u>	OIPC	410, 9925 - 109 Street and OIPC Website

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health System
2.0	June 2, 2010	ICAU Unit	ICAU	Performance and Information
				Management
			Linda Miller,	Todd Heron, ADM Health Accountability
1.0	June 13, 2003	RAPS Unit	Director IM	Division
			Branch	DIVISION

Contracting 40

IM POLICY 019 June 2, 2010

Research

Policy Statement

The Planning and Performance Branch coordinates the disclosure of individually and/or potentially identifiable health information for research purposes for Alberta Health and Wellness (AHW), in order to ensure that all disclosures for research comply with the *Health Information Act* (HIA) and other relevant legislation.

Purpose

This policy helps to ensures that the disclosure of individually identifying health information to researchers for academic, applied or scientific health-related purposes complies with the HIA and other relevant legislation.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - o Students
 - Information managers
- This policy applies to individually identifying diagnostic, treatment or care information or individually identifying registration information, or both, that may be disclosed to a researcher for research purposes. However, it excludes all disclosures to individuals who are the subject of the information being disclosed (e.g., HIA access requests, statement of benefits paid, ACHIP/Premiums issues); consented disclosures to third parties; all routine and/or publicly funded available data products or other summarized aggregate data products; and direct/live access to electronic data sources in the custody or under the control of AHW.

Compliance with Policy Statement

- Contact Health Information and Analysis Branch for assistance.
- Other program areas may respond to such requests, but must consult with Health Information and Analysis Branch before disclosing health information for research purposes.
- The Information Compliance and Access Unit (ICAU) will provide advice on the disclosure of information for research if required. Contact the HIA help desk at 780-427-8089 or <u>hiahelpdesk@gov.ab.ca</u>.

Research 41

IM POLICY 019 June 2, 2010

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with sections 48-56 of the HIA.

Linked documents	Owner	Location
Chapters 5 and 8 of the HIA	ICAU	21 st Floor, TPNT and
Guidelines and Practices Manual	ICAU	AHW Public Website
Research Data Disclosure Guidelines	Research & Evidence	
	Branch	
Research Data Access Handout	Research & Evidence	
	Branch	

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
2.0	June 2, 2010	ICAU	ICAU	System Performance and
				Information Management
1.0	luno 12, 2002	ICAU	Linda Miller Director IM	Todd Heron ADM Health
1.0	June 13, 2003	ICAU	Branch	Accountability Division

Research 42

IM POLICY 020 June 2, 2010

Information Manager Agreements

Policy Statement

The Information Compliance and Access Unit (ICAU) coordinates all information manager agreements (IMA) on behalf of Alberta Health and Wellness (AHW).

Purpose

AHW must ensure that all IMAs properly address the requirements set out in section 66 of the *Health Information Act* (HIA).

Applicable Groups and Assets

- AHW as custodian or as information manager
- Information managers, defined as a person or body that:
 - o processes, stores, retrieves or disposes of health information,
 - o in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information
 - provides information management or information technology services.
- · Health information in the custody or under the control of AHW
- All information manager agreements

Compliance with Policy Statement

- As per the HIA, third parties may act as information managers on behalf of AHW and AHW may act
 as an information manager on behalf of third parties. In either instance, ICAU will coordinate all
 IMAs to ensure that each IMA includes clauses that properly address the requirements set out in
 section 66 of the HIA.
- Contracts with information managers must include appropriate clauses as defined in section 66 of HIA. Appendix 4 of HIA Guidelines and Practices Manual provides guidance to this effect.
- Contracts with Information Managers located outside of Alberta must include additional clauses related to information security as described in section 8(4) of the Health Information Regulation.
- ICAU will consult with Legal and Legislative Services to ensure compliance with all relevant legislation.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA or FOIP. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA and FOIP,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with section 66 of the HIA.

IM POLICY 020 June 2, 2010

Linked documents	Owner	Location
Chapters 5, 9 and 11, and Appendix 4 of	ICAU	21 st Floor, TPNT and AHW
the HIA Guidelines and Practices Manual	ICAU	Public Website
Clauses for Contracts	ICAU	21 st Floor, TPNT and AHW
Clauses for Contracts	ICAU	Public Website
Public-sector Outsourcing & Risks to	OIPC	410, 9925 - 109 Street
<u>Privacy</u>	OIPC	OIPC Website
OIPC Investigation Reports <u>H2002-001</u> &	OIPC	410, 9925 - 109 Street
H2001-IR-009	UIFC	OIPC Website

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
2.0	June 2, 2010	ICAU	ICAU	System Performance and
				Information Management
1.0	June 13, 2003	RAPS Unit	Linda Miller Director IM Branch	Todd Heron ADM Health Accountability Division

IM POLICY 021 June 2, 2010

Provincial Courier

Policy Statement

Alberta Health and Wellness (AHW) as custodian should ensure that the applicable groups listed below are made aware that the provincial courier should be used when sending hard copies of individually identifying health information to and from AHW wherever the provincial courier service is available.

Purpose

To protect against any reasonably anticipated loss, unauthorized modification, misuse, or unauthorized destruction of hard copies of individually identifying health information exchanged between AHW and other organizations by using the provincial courier.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - Students
 - Information managers
- All individually identifying health information in hard copy format in the custody or under the control of AHW

Compliance with Policy

- AHW as custodian should ensure that applicable groups are made aware of the necessity to use the
 provincial courier as stated in this policy through any applicable information sharing agreements
 (ISA).
- Whenever appropriate, applicable groups must attend the mandatory HIA general awareness training which will inform them of the necessity to use the provincial courier as stated in this policy.

Health information is deemed to be confidential information as per the Information Security Classification and Control Standard. Therefore, all hard copies of health information sent via the provincial courier must adhere to security controls including:

- o Information must only be sent to a previously identified key contact at the intended destination;
- The Provincial Courier Registration Form must be accurately completed and filed for records purposes;
- o The information to be transported must be in a sealed opaque envelope, and;
- o Information being transported must be visibly classified as "Confidential" with a security or tamper-proof seal, and security and privacy disclaimer attached to it.

Provincial Courier 45

IM POLICY 021 June 2, 2010

If the provincial courier is not available other methods of distribution may be used. As much as possible, the same security control standards should be applied. Alternate forms of delivery include:

- Canada Post priority courier with signature required;
- Canada Post registered mail, and;
- o Any other courier company where the receiver signs to confirm delivery.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the *Health Information Act* (HIA). Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with the Information Security Classification & Controls Standards and section 60(1)(c) of the HIA.

Linked documents	Owner	Location
AHW <u>Information Security</u> <u>Classification & Control Standards</u>	Information Compliance and Access Unit (ICAU)	21 st floor, TPNT and AHW Public Website
Chapter 5 of the <u>HIA Guidelines</u> and Practices Manual	ICAU	21 st floor, TPNT and AHW Public Website

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
1.0	June 2, 2010	ICAU	ICAU	System Performance and
				Information Management

Provincial Courier 46

IM POLICY 022 June 2, 2010

Responding to requests to mask or remove information in Alberta Netcare

Policy Statement

Alberta Health and Wellness (AHW) has a duty to consider the expressed wishes of individuals who want their information masked in Netcare.

Purpose

Global Person-Level Masking (GPLM or "masking") is the mechanism through which the expressed wishes of an individual may be managed in Netcare. Under section 58(2) of the *Health Information Act* (HIA), AHW has a duty to consider expressed wishes. If an individual contacts AHW with a request to have his/her information in Netcare masked, then AHW must consider the expressed wishes of that individual by following the compliance section (below).

Applicable Groups and Assets

- AHW as a custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - Volunteers
 - o Students
 - o Information managers
 - o An individual's health information in Netcare

Compliance with Policy Statement

- When AHW receives calls from individuals, or authorized representatives, requesting that their
 information in Netcare be masked (or removed), the person receiving the call must transfer it to
 the HIA help desk (780-427-8089 or <a href="https://historian.nih.gov/histori
- An HIA policy advisor will consider individuals' expressed wishes by making a functional referral to individuals' physician, pharmacist and/or Alberta Health Services Information, Access and Privacy Coordinator. "Functional" refers to the requirement that the referral must be to a custodian in the health care delivery system who is able to address a masking request.
- An HIA policy advisor will inform callers that they should contact the HIA help desk if they experience difficulty in contacting a participating custodian, as per the referral.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with section 58(2) of the HIA.

IM POLICY 022 June 2, 2010

Linked documents	Owner	Location
Chapter 5 and 8 of the <u>HIA Guidelines and</u> <u>Practices Manual</u>	ICAU	21 st floor, TPNT and AHW Public Website
Alberta Netcare Electronic Health Record Information Exchange Protocol (Version 2.1)	AHW	21 st floor, TPNT
Guideline for Application for Global Person-Level Masking	AHW	21 st floor, TPNT
Application for Global Person-Level Masking Form	AHW	21 st floor, TPNT
Guideline for Authorization to Rescind Global Person-Level Masking	AHW	21 st floor, TPNT
Authorization to Rescind Global Person-Level Masking Form	AHW	21 st floor, TPNT

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM, Health
1.0	June 2, 2010	ICAU	ICAU	System Performance and
				Information Management

IM POLICY 023 June 2, 2010

Privacy Impact Assessments

Policy Statement

Alberta Health and Wellness (AHW) must prepare and submit a Privacy Impact Assessment (PIA) to the Office of the Information and Privacy Commissioner (OIPC) before implementing any proposed new information system or administrative practice that collects uses or discloses individually identifying health information, or any proposed change to existing practices and systems.

Purpose

PIAs are an exercise in due diligence that assures health system stakeholders and Albertans that AHW has identified and mitigated privacy and security concerns related to new systems and administrative practices. Section 64 of the *Health Information Act* (HIA) explains a custodian's duty to prepare privacy impact assessments.

The *Freedom of Information and Protection of Privacy Act* (FOIP) does not necessitate PIAs; however, they should be considered whenever collecting, using or disclosing personal information.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - Contractors/vendors
 - o Agents
 - Appointees
 - Volunteers
 - o Students
 - o Information managers
- This policy applies to all proposed administrative practices (including business processes, procedures, and related forms) and information systems (including applications and databases) relating to the collection, use and disclosure of individually identifying information and also applies to modifications to existing systems and/or administrative practices.

Compliance with Policy Statement

- The Information Compliance and Access Unit (ICAU), Privacy Team, facilitates the PIA process for AHW and for any provincial initiatives which AHW is the leader. This process is undertaken in consultation with relevant program areas/stakeholders. AHW affiliates engaged in new system development or proposing changes to existing system or administrative processes should contact the AHW Privacy Manager at 780-422-8642 to determine if a PIA is required.
- PIAs will be reviewed by Legal and Legislative Services and signed off by the Deputy Minister prior to submission to the OIPC.
- A PIA must be submitted to the OIPC prior to implementing a proposed information system or administrative practice relating to the collection, use or disclosure of individually identifying health information, or any proposed change to existing practices or systems.
- If a PIA has been accepted by the OIPC and an administrative practice or system change occurs, a new PIA may not always be required. Rather, a PIA addendum may be filed to capture these changes. Contact the AHW Privacy Manager at 780-422-8642 to determine if a PIA is required.

Privacy Impact Assessments 49

IM POLICY 023 June 2, 2010

• If a research proposal has been approved by an HIA designated Research Ethics Board (REB) and AHW has entered into an agreement with the researcher, a PIA would not be required. However, AHW has the authority to impose additional conditions on the researcher, which could also stipulate that a PIA would need to be completed prior to the disclosure of health information to the researcher. For additional information, refer to the policy, Privacy Impact Assessments for Data Matching for Research Purposes.

• In the event that a FOIP PIA is necessary, the ICAU Unit will assume the lead and the FOIP/HIA Office will provide support on the processing of the PIA and submission to the OIPC.

Alignment

This policy statement aligns with section 64 of the HIA.

Deviations from Policy

When the new information system or administrative practice or change to an existing practice or system, must be implemented before formal acceptance of the PIA or PIA Addendum is received from the OIPC, a deviation from the policy may occur with all of the following restrictions:

- 1. The PIA or PIA Addendum has been submitted to the OIPC,
- 2. The program area has demonstrated a need to proceed with implementation before PIA or PIA Addendum acceptance,
- 3. The risk would need to be assessed on an individual basis and ultimately, it would be at the responsibility of the program area, and
- 4. The exception must be approved by the AHW Privacy Manager.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA or FOIP. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA and FOIP,
- o disciplinary action for AHW affiliates.

Privacy Impact Assessments 50

IM POLICY 023 June 2, 2010

Linked documents	Owner	Location
Privacy Impact Assessment Guidelines	ICAU	21 st floor, TPNT and
Privacy impact Assessment Guidelines		AHW Public Website
Chapter 5 of the HIA Guidelines and	ICALL	21 st floor, TPNT and
Practices Manual	ICAU	AHW Public Website

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM,
2.0	luno 2 2010	ICALI	ICAU	Health System Performance
2.0	June 2, 2010	10 ICAU		and Information
				Management
1.0	June 13,		Linda Miller – Director IM	Todd Heron – ADM Health
1.0	2003		Branch	Accountability Division

Privacy Impact Assessments 51

IM POLICY 024 June 2, 2010

Privacy Impact Assessments for Disclosure for Health System Purposes

Policy Statement

Alberta Health and Wellness (AHW) as custodian and all AHW affiliates must submit a Privacy Impact Assessment (PIA) to the Office of the Information and Privacy Commissioner (OIPC) before requesting a disclosure of individually identifying health information from another custodian for health system purposes.

Purpose

A PIA is an exercise in due diligence that assures health system stakeholders that AHW has identified and mitigated privacy and security concerns related to disclosures of individually identifying health information for health system purposes. This policy ensures compliance with section 46(5) of the *Health Information Act* (HIA).

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - o Contractors/vendors
 - Agents
 - o Appointees
 - o Volunteers
 - Students
 - Information managers
- Individually identifying health information requested by the Minister or the Department from another custodian for any of the purposes listed in section 27(2) of the HIA and that relates to a health service provided by the other custodian and (i) the health service is fully or partially paid for by the Department or is provided using financial, physical or human resources provided, administered or paid for by the department, or (ii) the information is prescribed in the regulations as information the Minister or the Department may request under this section.

Compliance with Policy Statement

- AHW affiliates that are requesting a disclosure of individually identifying health information from another custodian for health system purposes should contact the HIA help desk at 427-8089 or hiahelpdesk@gov.ab.ca to determine if a PIA is required.
- The Information Compliance and Access Unit (ICAU), Privacy Team, facilitates the PIA process for AHW. This process is undertaken in consultation with relevant program areas/stakeholders.
- PIAs must be reviewed by Legal and Legislative Services (LLS) and signed off by the Deputy Minister (DM) prior to submission to the OIPC.
- A PIA must be submitted to the OIPC prior to requesting a disclosure of individually identifying health information from another custodian for health system purposes.

IM POLICY 024 June 2, 2010

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- public investigations and Orders by the Office of the Information and Privacy Commissioner,
- fines under the HIA,
- disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with section 46(5) of the HIA.

Linked documents	Owner	Location
Privacy Impact Assessment Guidelines	ICAU	21 st floor, TPNT
	ICAU	and AHW Public Website
Chantar Q of the LIIA Cuidelines and		21 st floor, TPNT
hapter 8 of the HIA Guidelines and	ICAU	and AHW
Practices Manual		Public Website

Version	Date	Author	Reviewers	Approval
				Mark Brisson, A/ADM,
				Health System
2.0	2.0 June 2, 2010	ICAU	ICAU	Performance and
				Information
				Management
			Linda Miller – Director IM	Todd Heron – ADM
1.0 June 13, 2003		Branch	Health Accountability	
			Diancii	Division.

IM POLICY 025 June 2, 2010

Privacy Impact Assessments for Data Matching

Policy Statement

Alberta Health and Wellness (AHW) must prepare a Privacy Impact Assessment (PIA) and submit the assessment to the Office of the Information and Privacy Commissioner (OIPC) for review before performing data matching with other custodians or with non-custodians.

<u>Purpose</u>

A PIA is an exercise in due diligence that assures health system stakeholders that AHW has identified and mitigated privacy and security concerns related to data matching. "Data matching" means the creation of individually identifying health information by combining individually identifying or non-identifying health information or other information from 2 or more electronic databases, without the consent of the individuals who are the subjects of the information (section 1(1)(g)). This policy ensures compliance with sections 70 and 71 of the *Health Information Act* (HIA).

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - o Students
 - o Information managers
- All health information in the custody or under the control of AHW that is to be used in data matching or health information that is created through data matching.

Compliance with Policy Statement

- The Information Compliance and Access Unit (ICAU), Privacy Team, facilitates the PIA process for AHW in consultation with relevant program areas/stakeholders. AHW affiliates engaged in data matching must contact the AHW Privacy Manager at 780-422-8642 to determine if a PIA is required.
- PIAs will be reviewed by Legal and Legislative Services and signed off by the Deputy Minister prior to submission to the OIPC.
- A PIA must be submitted to the OIPC before the data matching activity can be performed.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with sections 69, 70 and 71 of the HIA.

IM POLICY 025 June 2, 2010

Deviations from Policy

When data matching occurs before formal acceptance of the PIA or PIA Addendum is received from the OIPC, a deviation from the policy may occur with all of the following restrictions:

- 1. The PIA or PIA Addendum has been submitted to the OIPC,
- 2. The program area has demonstrated a need to proceed with data matching before PIA or PIA Addendum acceptance,
- 3. The risk would need to be assessed on an individual basis and ultimately, it would be at the responsibility of the program area, and
- 4. The exception must be approved by the AHW Privacy Manager in consultation with the Assistant Deputy Minister of Health System Performance and Information Management Division.

Linked documents	Owner	Location
Privacy Impact Assessment Guidelines	ICAU	21 st floor, TPNT and AHW Public Website
Chapter 5 of the HIA Guidelines and Practices Manual	ICAU	21 st floor, TPNT and AHW Public Website

Version	Date	Author	Reviewers	Approval
		ICAU	ICAU	Mark Brisson, A/ADM,
				Health System
2.0	2.0 June 2, 2010			Performance and
				Information
				Management
		Linda Miller – Director IM Branch	Todd Heron – ADM	
1.0 June 13, 2003			Health Accountability	
			Division	

IM POLICY 026 June 2, 2010

Privacy Impact Assessments for Data Matching for Research Purposes

Policy Statement

When data matching is performed for the purpose of conducting research, Health Information and Analysis Branch must determine whether a Privacy Impact Assessment (PIA) is required prior to disclosing the information.

Purpose

A PIA is an exercise in due diligence that assures health system stakeholders that Alberta Health and Wellness (AHW) has identified and mitigated privacy and security concerns related to data matching related to research subject to section 72 of the *Health Information Act* (HIA).

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - o AHW employees
 - Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - Students
 - Information managers
- All health information to be used in the data matching for research purposes or created through data matching for research purposes.

Compliance with Policy Statement

- The AHW Health Information and Analysis Branch, is the only AHW business area that may provide data to researchers. This helps to ensure that due diligence is exercised by having only that business area determine if a PIA is required for research purposes.
- The AHW Health Information and Analysis Branch, will consult with the Information Compliance and Access Unit (ICAU), Privacy Team, on any projects that may require a PIA to ensure best practice in data matching for research.
- If a PIA is required, it will be filed with ICAU, Privacy Team, before data matching for research can be performed.
- The AHW Planning and Performance Branch, in consultation with the ICAU,,Privacy Team, may determine when a PIA is not required.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA,
- o disciplinary action for AHW affiliates.

IM POLICY 026 June 2, 2010

<u>Alignment</u>

This policy statement aligns with section 72 of the HIA.

Linked documents	Owner	Location
Privacy Impact Assessment Guidelines	ICAU	21 st floor, TPNT and
	ICAU	AHW Public Website
Chapter 5 of the HIA Guidelines and	ICAU	21 st floor, TPNT and
Practices Manual	ICAU	AHW Public Website

Version	Date	Author	Reviewers	Approval
		une 2, 2010 ICAU		Mark Brisson, A/ADM,
				Health System
2.0	2.0 June 2, 2010		ICAU	Performance and
				Information
				Management
		13, 2003	Linda Miller – Director IM	Todd Heron – ADM
1.0 June 13, 2003	June 13, 2003			Health Accountability
		Branch		Division

IM POLICY 027 June 2, 2010

Access to Data Holdings Process

Policy Statement

The access to data holdings process must be completed before Alberta Health and Wellness (AHW) as custodian allows its affiliates to access and use health information from AHW data holdings.

Purpose

The access to data holdings process is a safeguard that helps to ensure that AHW as custodian and its affiliates adhere to the principles of "highest degree of anonymity," "least amount of information" and "need to know" when requesting access to or using AHW data holdings.

Applicable Groups and Assets

- AHW as custodian
- All AHW affiliates (may include but not necessarily be limited to):
 - AHW employees
 - Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - Students
 - Information managers
- Subject to exceptions set out in HIA and FOIP, all health information in the custody or under the control of AHW.

Compliance with Policy

- Contact the access to data holdings administrator with any questions or to request access to data holdings at A2DHadmin@gov.ab.ca.
- Affiliates who require access to data holdings must apply for access to that information by
 considering the highest degree of anonymity, using the least amount of information and based on a
 need to know in order to complete the intended task at hand.
- When following the access to data holdings process, ensure that all steps are followed accurately and that all necessary approvals are met with.
- Do not continue to access and use data holdings after access is no longer necessary. Inform the
 access to data holdings administrator that you no longer require access to the data holdings you
 are no longer using.

Deviations to Policy

All deviations must be approved by the AHW Privacy Manager, Information Compliance and Access Unit (ICAU) and the AHW Executive Director, Information Management Branch.

IM POLICY 027 June 2, 2010

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA. Failure to comply with this policy may result in:

- public investigations and Orders by the Office of the Information and Privacy Commissioner,
- fines under the HIA,
- disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with sections 57 and 58 of the HIA.

Linked documents	Owner	
Access to Data Holdings Process	ICAU	21 st floor, TPNT and
Access to Data Holdings Process		AHW Public Website
Access to Data Holdings Application	ICAU	21 st floor, TPNT and
Access to Data Holdings Application		AHW Public Website

Version	Date	Author	Reviewers	Approval
2.0	June 2, 2010	ICAU	ICAU	Mark Brisson, A/ADM, Health System Performance and
2.0	3dile 2, 2010	16,10	16,16	Information Management
1.0	June 13, 2003		Linda Miller – Director IM Branch	Todd Heron – ADM Health Accountability Division

IM POLICY 028 June 2, 2010

Privacy Breaches

Policy Statement

Alberta Health and Wellness (AHW) as custodian and all AHW affiliates must report all privacy breaches, as soon as possible, to the Manager of Privacy, Information Compliance and Access Unit (ICAU), AHW via the HIA help desk at 780-427-8089 or ahw.security@gov.ab.ca.

Purpose

The privacy breach reporting procedure enables AHW to appropriately review, investigate and rectify any potential or actual privacy issue. Privacy breaches indicate gaps in a custodian's or an affiliate's ability to safeguard information in accordance with the *Health Information Act* (HIA) or the *Freedom of Information and Protection of Privacy* (FOIP) Act.

Applicable Groups and Assets

- AHW as custodian and as a public body
- All AHW affiliates (may include but not necessarily limited to):
 - o AHW employees
 - o Contractors/vendors
 - o Agents
 - o Appointees
 - o Volunteers
 - Students
 - o Information managers
- All information in the custody or under the control of AHW

Compliance with Policy Statement

If you suspect that a privacy breach has occurred:

- Inform your supervisor of the privacy breach, as soon as possible.
- Fill out a "Privacy and Security Incident Reporting" Form (linked below).
- Contact the Manager of Security, ICAU, AHW (427-8089) and notify him/her of the privacy breach. The Privacy Manager is responsible for initiating an appropriate response to the breach.

Penalties and Consequences

This policy ensures that AHW complies with and is not in breach of the HIA or FOIP. Failure to comply with this policy may result in:

- o public investigations and Orders by the Office of the Information and Privacy Commissioner,
- o fines under the HIA and FOIP,
- o disciplinary action for AHW affiliates.

Alignment

This policy statement aligns with section 63(1) of the HIA and FOIP.

Linked documents	Owner	Location	
Privacy Impact Assessment Guidelines	ICAU	21 st floor, TPNT and AHW	
Filvacy impact Assessment duidennes	ICAU	Public Website	
AHW Information Security Policy Manual	ICAU	21 st floor, TPNT and AHW	

Privacy Breaches 60

IM POLICY 028 June 2, 2010

		Public Website
Privacy and Security Incident Reporting Form	ICAU	21 st floor, TPNT and AHW Public Website

Version	Date	Author	Reviewers	Approval
2.0	June 2, 2010	ICAU	ICAU	Mark Brisson, A/ADM, Health System Performance and Information Management
1.0	June 13, 2003		Linda Miller – Director IM Branch	Todd Heron – ADM Health Accountability Division

Privacy Breaches 61

Alberta Health and Wellness Provincial Health Information Executive Committee (HIEC)

Terms of Reference

This document defines the Terms of Reference (ToR) of the Provincial Health Information Executive Committee and was approved on June 22, 2009 by the Deputy Minister, Alberta Health and Wellness.

Purpose and Scope

The Provincial Health Information Executive Committee is an executive, authoritative committee with the mandate to provide strategic leadership, set provincial priorities, approve strategic-level impact initiatives which define scope, budget and timelines and address inter-organizational issues where necessary for Alberta's Electronic Health Record (EHR) and intersections related to publicly funded IM/IT health sector initiatives. The Provincial Health Information Executive Committee reports to the Minister of Health.

Responsibilities

The Provincial Health Information Executive Committee will be responsible for:

- Approving the terms of reference for the following committees:
 - Information Management / Information Technology (IM/IT) Strategy Committee;
 - o The EHR Sponsors Committee; and
 - o Initiative Steering Committees (generic mandate).
- Providing strategic direction to health sector Information Management/Information Technology (IM/IT) leadership in managing EHR investments;
- Approving the three-year strategic plan for the provincial EHR and related health systems initiatives;
- Providing strategic direction to related initiatives that directly impact the EHR and other provincial initiatives;
- Supporting and guiding the Electronic Health Record Data Stewardship Committee (EHRDSC) in understanding the EHR/EMR information priorities;
- Ensuring that provincial strategies are aligned with, and take full advantage of, national and inter-jurisdictional initiatives; and
- Ensuring that a coordinated provincial communications strategy is in place for provincial EHR and related health initiatives.

Membership

The Provincial Health Information Executive Committee will be comprised of the following voting members:

- The Deputy Minister, Alberta Health and Wellness
- Chief Executive Officer (CEO), Alberta Health Services
- Assistant Deputy Minister, Health System Performance and Information Management Division, Alberta Health and Wellness
- Executive Director, Alberta Medical Association
- Chief Information Officer, Alberta Health Services
- Chief Medical Officer, Alberta Health Services
- Registrar, Alberta College of Pharmacists

Each member is empowered to vote individually on behalf of the stakeholder organization they represent on any motion raised at the Provincial Health Information Executive Committee.

The committee is chaired by the Deputy Minister. A consistent alternate will be designated by the Chair, from the current membership list. The Chair is responsible for:

- Setting and approving meeting agenda;
- Arranging additional meetings as required;
- Facilitating meetings;
- Assigning or delegating tasks; and
- Ensuring accountability of tasks.

Members are appointed to the committee for two years, with eligibility for reappointment. New members may be added at the discretion of the Chair. Member resignation and/or replacement are also at the discretion of the Chair.

Members may send a delegate to any meeting, upon notifying the Chair by e-mail.

A current membership list is attached as Appendix A.

Principles of Operation

The Provincial Health Information Executive Committee will operate under a published set of principles, which may be amended from time to time by agreement of the members, and approval of the Deputy Minister. Current principles are attached as Appendix B.

Administrative Support

The Provincial Health Information Executive Committee will be supported by secretariat services provided by AHW's CIO as per the guidelines in the Meeting Procedures.

Meeting Procedures

The Provincial Health Information Executive Committee will:

- Meet every ten (10) weeks, or at the call of the Chair. Ad-hoc meetings may from time to time be required, and where possible, these will be arranged by video conference, telephone conference, or via such means as to minimize time demands on the members:
- Ensure regular meetings are scheduled at least six weeks in advance;
- Ensure meetings are held at such dates, times and locations as to be efficient to the requirements of its members;
- Ensure meetings are called by the Chair, or the Chair's designate;
- Ensure agendas are set with input from the members, but at the final discretion of the Chair;
- Ensure agenda and appropriate supporting documentation are distributed five working days in advance of each meeting or workshop;
- Ensure that presentations by non-members are scheduled by agreement of members and the Chair; and
- Ensure minutes of each meeting, and decisions made, are recorded and distributed to all attendees and all members, via e-mail, within five working days of the meeting. Members will be responsible to review the minutes and distributed

materials within ten working days of receipt and notify the secretariat services of any errors or omissions. Finalized minutes and decisions will be posted to a location accessible to all members.

Quorum

Attendance of two-thirds of the members will be required to conduct a meeting.

Decision Making

Wherever possible, all decisions of the Provincial Health Information Executive Committee will be made by consensus. Where this is not possible, a vote will be called by the Chair, whereby:

- Each member shall have one vote; and
- A two-thirds majority vote will carry a motion.

Success Criteria

The evaluation framework listed below will be used to measure committee success. Data will be compiled on a monthly basis, by the administrative support person. Compiled reports will be distributed to committee members for validation prior to distribution to the Minister of Health.

Criterion	Indicators	Data Sources	Data Collection Approach
Oversight of IM/IT governance model	% of current committees with Terms of Reference approved by HIEC.		
Provision of strategic direction to health sector IM/IT leadership	Response time for addressing requests for IM/IT direction		
Clear understanding of provincial EHR strategies	Dissemination status of 3-year Integrated IM/IT Strategy		

Appendix A: Membership List

Voting Members

Person (role)	Organization / Functional Area	Position	Appointment Term
Linda Miller (Chair)	Alberta Health and Wellness	Deputy Minister	
Stephen Duckett	Alberta Health Services	Chief Executive Officer (CEO)	
Mike Conroy	Alberta Health Services	Executive VP, Corporate Services	
Bill Trafford	Alberta Health Services	Chief Information Officer (CIO)	
Mike Gormley	Alberta Medical Association	Executive Director	
Dr. Brenda Bunting, (Alternate)			
Mark Brisson	Alberta Health and Wellness	Acting Assistant Deputy Minister, Health System Performance and Information Management Division	
Greg Eberhart	Alberta College of Pharmacists	Registrar	

Non-Voting Members

None

Appendix B: Principles of Operation

The Provincial Health Information Executive Committee will operate under the following principles:

- 1. This Committee will determine strategy, not conduct analysis.
- 2. This Committee will deal with strategic issues related to the investment in and overall direction of Alberta's EHR and component provincial initiatives, (eg. Electronic Medical Records).
- 3. This Committee will resolve issues escalated from the EHR Sponsors Committee, EHR Data Stewardship Committee and IM/IT Strategy Committee.
- 4. This group will not deal directly with any supplier organization.
- 5. All issues before this Committee will be presented in context of the Alberta health system, using health system business language. Any items brought before this Committee that are presented in technical jargon may be rejected.
- 6. All recommendations made by this Committee will be arrived at via an open and transparent process, and be communicated to appropriate stakeholders via an approved communications plan.
- 7. Membership of this Committee, and its operating principles and processes, will be open to continuous re-evaluation by its members.
- 8. Any changes made to this document will be at the discretion of the Committee and will be forwarded to the Governance Coordinating Unit for filing.
- 9. Should urgent matters arise between scheduled meetings, the Chair may conduct an e-mail vote/poll of members. These decisions will be reflected in the agenda and minutes of the next official meeting.

Alberta Health and Wellness Information Management/Information Technology (IM/IT) Strategy Committee

Terms of Reference

This document defines the Terms of Reference (ToR) of the Information Management/ Information Technology (IM/IT) Strategy Committee and was approved on June 22, 2009, by the EHR Governance Committee.

Purpose and Scope

The IM/IT Strategy Committee is an advisory committee to the Health Information Executive Committee and has the mandate to develop 3-year strategic plans for the Electronic Health Record (EHR) and related e-Health initiatives updated annually, as well as to function as a provincial forum for healthcare Information Management and Information Technology (IM/IT) policy advice. The IM/IT Strategy Committee reports to the Health Information Executive Committee (HIEC), and recommends the IM/IT strategic plans to HIEC for adoption.

Responsibilities

The IM/IT Strategy Committee is responsible for:

- Approving assigned Terms of Reference for strategy task groups and other steering committees as assigned;
- Developing and maintaining a regular review of the 3 -5 year Provincial IM/IT
 e-Health Integrated Strategic Plan with visibility of participating organizations plans
 reflected within the integrated IM/IT plan;
- Recommending information sharing, privacy and security policies;
- Promoting with key stakeholders the understanding and best practices for the management of information within the health system;
- Providing guidance to EHR and other related initiatives on Provincial IM/IT e-Health Strategy; and
- Providing input into the development and implementation of a provincial e-Health communications strategy and plan.

Membership

The IM/IT Strategy Committee is comprised of the following Members, as appointed by the Chair:

Voting

- CIO, Alberta Health and Wellness (AHW), (Chair);
- Executive Director for EHR Development and Delivery, Alberta Health and Wellness;
- CIO, Alberta Health Services;
- One representative appointed by CIO, Alberta Health Services;
- One physician representative, Alberta Medical Association;
- One representative, College of Physicians and Surgeons of Alberta;
- One pharmacist representative, Alberta College of Pharmacists;
- One representative, College and Association of Registered Nurses of Alberta; and
- One representative, Service Alberta, Government of Alberta.

Non-voting

- Executive Director, Information Management, Alberta Health and Wellness;
- One representative, Health System Performance and Information Management Division, Alberta Health and Wellness; and
- One representative, Office of the Information and Privacy Commissioner for Alberta.

Each voting member is empowered to vote on behalf of the stakeholder organization they represent on any motion raised at the IM/IT Strategy Committee.

The committee is chaired by the Assistant Deputy Minister, Health System Performance and Information Management Division, and CIO, Alberta Health and Wellness. A consistent alternate will be designated by the Chair from the current membership list. The Chair is responsible for:

- Setting and approving meeting agenda;
- Arranging additional meetings as required;
- Facilitating meetings;
- Assigning or delegating tasks; and
- Ensuring accountability of tasks.

Members are appointed to the committee for two or three years, with eligibility for reappointment. Membership terms will be staggered, to avoid complete turnover at any renewal date. New members may be added at the discretion of the Chair. Member representation and/or replacement are also at the discretion of the Chair.

Members may send a delegate to any meeting, with full voting rights, upon notifying the Chair by e-mail.

Members may elect to grant their vote to another member by proxy, by notifying the Chair and the proxy member by e-mail.

A current membership list is attached as Appendix A.

Principles of Operation

The IM/IT Strategy Committee will operate under a published set of principles, which may be amended from time to time by agreement of the Members, and approval of the Chair. Current principles are attached as Appendix B.

Administrative Support

The IM/IT Strategy Committee will be supported by secretariat services provided by AHW, as per the guidelines in the Meeting Procedures.

Meeting Procedures

The IM/IT Strategy Committee will:

- Meet regularly on a bi-monthly basis, at the discretion of the Chair, or as needed for strategic planning in support of the development of strategic plans and priorities.
 Ad-hoc meetings may from time to time be required, and where possible, these will be arranged by video conference, telephone conference, or via such means as to minimize time demands on the Members;
- Ensure regular meetings are scheduled at least six weeks in advance;
- Ensure meetings are held at such dates, times and locations as to be efficient to the requirements of its Members;

- Ensure meetings are called by the Chair, or the Chair's designate;
- Ensure agenda are set with input from the members, but at the final discretion of the Chair;
- Ensure agenda and appropriate supporting documentation are distributed five working days in advance of each meeting or workshop;
- Ensure that presentations by non-Members are scheduled by agreement of members and the Chair; and
- Ensure minutes of each meeting, and decisions made, are recorded and distributed
 to all attendees and all Members, via e-mail, within five working days of the
 meeting. Members will be responsible to review the minutes and distributed
 materials within ten working days of receipt and notify the secretariat services of any
 errors of omissions. Finalized minutes and decisions will be posted to a location
 accessible to all Members.

Quorum

Attendance of two-thirds of the members, in person or by proxy, will be required to conduct a meeting.

Decision Making

Wherever possible, all decisions of the IM/IT Strategy Committee will be made by consensus. Where this is not possible, a vote will be called by the Chair, whereby:

- Each member shall have one vote; and
- A two-thirds majority vote will carry a motion.

Success Criteria

Success of the IM/IT Strategy Committee will be evident by:

- Approval of an Integrated Strategy Plan by Health Information Executive Committee
- E-Health User Survey (annual) reflects confidence in direction of e-health strategy

The evaluation framework listed below will be used to measure committee success. Data will be compiled on a monthly basis, by the administrative support person. Compiled reports will be distributed to committee members for validation prior to distribution to the Provincial Health Information Executive Committee.

Evaluation Framework

Evaluation Framework				
Activities	Expected Outcomes	Indicators	Data Sources	Data Collection Approach

Appendix A: Membership List

Voting Members

Person (role)	Organization / Functional Area	Position	Appointment Term
Mark Brisson (chair)	Alberta Health and Wellness	Acting Assistant Deputy Minister, Health System Performance and Information Management Division, and CIO	
Belinda Boleantu	Alberta Health Services	VP IT - Clinical Transformation Services	
Kathleen Addison	Alberta Health Services	VP, Patient Information Services	
Fraser Armstrong Victor Taylor (Alternate)	Alberta Medical Association	Physician representative	
Dr. Jim Bell	College of Physicians and Surgeons of Alberta		
Greg Eberhart Dale Cooney (Alternate)	Alberta College of Pharmacists	Pharmacist representative	
Debra Allen	College and Association of Registered Nurses of Alberta		
Dan Sheplawy	Alberta Health and Wellness	Executive Director for EHR Development and Delivery	
Cherie Freeman	Service Alberta, Government of Alberta		
Laurel Frank (Alternate)			

Non-Voting Members

Person (role)	Organization / Functional Area	Position	Appointment Term
Susan Anderson	Alberta Health and Wellness	Acting Executive Director, Information Management	
Steven Long	Alberta Health and Wellness	Health System Performance and Information Management Division, representative	
LeRoy Brower	Office of the Information and Privacy Commissioner for Alberta	Representative	

^{*}alternate member

Appendix B: Principles of Operation

The IM/IT Strategy Committee will operate under the following principles:

- 1. This Committee will be used to conduct analysis, evaluate alternatives, and formulate strategies and plans for approval by the Provincial Health Information Executive Committee.
- 2. This Committee will deal with business issues and strategic planning related to the investment in management of Information Management/Information Technology in the broad health sector.
- 3. This Committee will escalate unresolved issues to the Provincial Health Information Executive Committee.
- 4. This Committee will not deal directly with any supplier organization.
- 5. All decisions reached by this Committee will be arrived at via an open and transparent process, and be communicated to appropriate stakeholders via an approved communications plan.
- 6. Membership of the Committee, and its operating principles and processes, are open to continuous re-evaluation by its Members.
- 7. Any changes made to this document will be at the discretion of the Committee and will be forwarded to the Governance Coordinating Unit for filing.
- 8. Should urgent matters arise between scheduled meetings, the Chair may conduct an email vote/poll of members. These decisions will be reflected in the agenda and minutes of the next official meeting.

Alberta Health and Wellness Electronic Health Record (EHR) Sponsors Committee

Terms of Reference

This document defines the Terms of Reference (ToR) of the Electronic Health Record (EHR) Sponsors Committee and was approved on June 22, 2009 by the EHR Governance Committee.

Purpose and Scope

The Electronic Health Record (EHR) Sponsors Committee has the mandate to ensure the strategic direction provided by the Health Information Executive Committee is achieved, by providing executive oversight (leadership, management, progress monitoring and issue resolution) for provincially funded e-Heath initiatives reporting to the EHR Sponsors Committee. The EHR Sponsors Committee is an advisory committee reporting to the Health Information Executive Committee.

Responsibilities

The EHR Sponsors Committee will be responsible for:

- Approving specific terms of reference for initiative-level steering committees that report up the EHR Sponsors Committee;
- Providing leadership to assigned EHR initiatives by ensuring business objectives of the assigned initiatives are being met within approved scope, budget and timelines, and risk mitigation plans are in place and actively managed;
- Monitoring progress of assigned initiatives by ensuring strategic level interdependencies between initiatives are being addressed, and resolve interorganizational issues where necessary;
- Reporting progress of assigned EHR initiatives to the Health Information Executive Committee, including identification of potential risks, strategic issues, mitigation strategies and recommendations for required action;
- Liaising with IM/IT Strategy Committee, EHR Data Stewardship Committee and other related committees by ensuring related committees are apprised of EHR direction and progress relative to respective committee mandates; and
- Ensuring initiative-specific progress and communication plans are developed in accordance with approved provincial communication strategies.

Membership

The EHR Sponsors Committee will be comprised of the following voting members:

- Two members, Alberta Health Services, including the CIO or equivalent;
- Two members, Alberta Medical Association including one primary care or PCN lead Physician;
- One member, College of Physicians and Surgeons;
- One member, Alberta Pharmacists Association; and,
- Two members, Alberta Health and Wellness, including the CIO for AHW.

The EHR Sponsors Committee will be comprised of the following non-voting members:

Executive Director for EHR, Alberta Health and Wellness; and

• Chair or Executive Lead of the reporting Steering Committees (attendance as required and limited by agenda).

Each member is empowered to vote individually on behalf of the stakeholder organization that they represent on any motion raised at the EHR Sponsors Committee.

The committee is Co-Chaired by AHS and AHW. The Co-Chairs are responsible for:

- Setting and approving meeting agendas;
- Arranging additional meetings as required;
- Facilitating meetings;
- Assigning or delegating tasks; and
- Ensuring accountability of tasks.

Members are appointed to the committee for two years, with eligibility for reappointment. New members may be added at the discretion of the Co-Chairs. Member resignation and/or replacement are also at the discretion of the Co-Chairs.

Members may send a delegate to any meeting in lieu of attendance, upon notifying one of the Co-Chairs by e-mail.

The Current Membership list is attached as Appendix A.

Principles of Operation

The EHR Sponsors Committee will operate under a published set of principles, which may be amended from time to time by agreement of the Members, and approval of the Deputy Minister. Current principles are attached as Appendix B.

Administrative Support

The EHR Sponsors Committee will be supported by secretariat services provided by AHW's CIO as per the guidelines in the Meeting Procedures.

Meeting Procedures

The EHR Sponsors Committee will:

- Meet every two weeks, or at the call of the Co-Chairs. Ad-hoc meetings may from time to time be required, and where possible, these will be arranged by video conference, telephone conference, or via such means as to minimize time demands on the Members:
- Set agendas with input from the members, but at the final discretion of the cochairs;
- Ensure meetings are conducted by one (or any) of the co-chairs or their designates;
- Ensure meetings are held at such dates, times and locations as to be efficient to the requirements of its Members;
- Ensure agendas and appropriate supporting documentation are distributed five working days in advance of each meeting or workshop;
- Ensure that presentations by non-Members are scheduled by agreement of members and the Chair; and
- Ensure minutes of each meeting, and decisions made, are recorded and distributed
 to all attendees and all Members, via e-mail, within five working days of the
 meeting. Members will be responsible to review the minutes and distributed
 materials within ten working days of receipt and notify the secretariat services of any

errors of omissions. Finalized minutes and decisions will be posted to a location accessible to all Members.

Quorum

Attendance of two-thirds of the members (in person or via teleconference or video conference) will be required to conduct a meeting. The chair has discretion of declaring if quorum is met.

Decision Making

Wherever possible, all decisions of the EHR Sponsors Committee will be made by consensus. Where this is not possible, a vote will be called by the chair, whereby:

- Each member shall have one vote; and
- A two-thirds majority vote will carry a motion.

If a vote fails or the issue remains unresolved, the issue (with two defined options) will be escalated to the Health Information Executive Committee for consideration.

Success Criteria

The evaluation framework listed below will be used to measure committee success. Data will be compiled on a monthly basis, by the administrative support person. Compiled reports will be distributed to committee members for validation prior to distribution to the Health Information Executive Committee.

Criterion	Indicators	Data Sources	Data Collection Approach
Timely response to decision requests	Response time for addressing decision requests		PMO & Delivery Manager
Timely and effective issues resolution process	Response time for addressing issues # of issues escalated to Health Information Executive Committee		Minutes of Health Information Executive Committee reflecting occurrences and time elapse.
Do underlying projects meet their success criteria: budget, time, quality outcome	Post project phase assessment		PMO & Delivery Manager, annual Netcare EHR User Survey

Appendix A: Membership List

Voting Members

Person (role)	Organization / Functional Area	Position	Appointment Term
Bill Trafford (Co-chair) Michael Long (Alternate)	Alberta Health Services	CIO or equivalent	2 years, Apr 2009 – March 2011
Claire McCrank	Alberta Health Services	Designated by CIO	2 years
Vic Taylor Mike Gormley (Alternate)	Alberta Medical Association	CIO or equivalent	2 years
Brendan Bunting	Alberta Medical Association	Primary Care Physician	2 years
John Swiniarski	College of Physicians and Surgeons	Executive Director	2 years
Keith Stewart	Alberta Pharmacy Association (RxA)	Executive Director	2 years
Mark Brisson (Co-chair)	Alberta Health and Wellness	Acting ADM/CIO	2 years
Susan Anderson	Alberta Health and Wellness	Acting Executive Director, Information Management	2 years

Non-Voting Members

Person (role)	Organization / Functional Area	Position	Appointment Term
Dan Sheplawy (Executive Director for EHR Development and Delivery)	AHW Netcare EHR	ED as ex-officio	
Chris Kearney	Registries Steering Committee	Chair or Executive Lead	
Dan Sheplawy	Diagnostic Imaging (DI) Steering Committee	Chair or Executive Lead	
Blaine Steward	Hub/Viewer Steering Committee	Chair or Executive Lead	
	Pharmacy Information Network (PIN) Stewardship Committee	Chair or Executive Lead	
	Personal Health Portal Steering Committee	Chair or Executive Lead	

^{*}alternate member

Appendix B: Principles of Operation

The AHW EHR Sponsors Committee will operate under the following principles:

- 1. This forum will deal with business issues related to the investment in and management of the Alberta EHR.
- 2. This forum will be the first level of escalation for unresolved issues that arise from the Steering Committees for which it is responsible.
- 3. This forum will not deal directly with any supplier organization.
- 4. All issues before this forum, will be presented in context of the Alberta health system, using health system business language.
- 5. All recommendations made by this forum, will be arrived at via an open and transparent process, and will be communicated to appropriate stakeholders via an approved communications plan.
- 6. Membership of the EHR Sponsors Committee, and its operating principles and processes, will be open to continuous re-evaluation by its members.
- 7. Any changes made to this document will be at the discretion of the EHR Sponsors Committee and will be forwarded to the Governance Coordinating Unit for filing.
- 8. Should urgent matters arise between scheduled meetings, the Chair may conduct an email vote/poll of members. These decisions will be reflected in the agenda and minutes of the next official meeting.



Alberta Health & Wellness Information Security Policy Manual

Written and maintained by: Information Policy and Compliance (IPC) Unit Information Management Branch Information Strategic Services Division July 2007



Commitment

Security is a responsibility shared by all Alberta Health and Wellness (AHW) employees, agents, and contractors. The Minister, Deputy Minister, and all Executives are committed to protecting the Confidentiality, Integrity, and Availability of AHW Information.



Table of Contents

I.	EXECUTIVE SUMMARY	1
II.	. INFORMATION SECURITY POLICY GOVERNANCE	1
	Introduction	1
	ORGANIZATION OF THE INFORMATION SECURITY POLICY MANUAL	
	GOAL AND OBJECTIVE	
	Information Security Principles.	
	DEFINITIONS AND ABBREVIATIONS	
	APPLICABLE GROUPS	
	STATEMENT OF APPLICABILITY	
	NON-COMPLIANCE AND DEVIATIONS	3
	ALIGNMENT	3
	OBLIGATIONS	3
	COMPLIANCE WITH POLICY	
	Information Security Development Process	
	Information Security Standards	
	ROLES AND RESPONSIBILITIES	
	REVIEW PERIOD	
	REVIEW PROCESS	
	Information Security Policy Manual Governance Section Version History	<i>6</i>
II	I. INFORMATION SECURITY POLICIES	7
O]	RGANIZATIONAL SECURITY POLICIES	7
	POLICY DIRECTIVE 1.0 - ORGANIZATIONAL SECURITY	7
	ISP 1.1 - Information Security Infrastructure	
	ISP 1.2 - Independent Review of Information Security.	
	ISP 1.3 - SECURITY OF THIRD PARTY ACCESS	
	ISP 1.4 - Outsourcing	
	ISP 1.5 – Security Policy Exceptions	
	NFORMATION AND CONTROL POLICIES	
	POLICY DIRECTIVE 2.0 - ASSET SECURITY CLASSIFICATION AND CONTROL	
	ISP 2.1 – ACCOUNTABILITY OF INFORMATION	
	ISP 2.2 – ACCOUNTABILITY OF BUSINESS PROCESSES	
	ISP 2.3 – Information Security Classification	
Ρŀ	ERSONNEL SECURITY POLICIES	18
	POLICY DIRECTIVE 3.0 - PERSONNEL SECURITY	
	ISP 3.1 – SECURITY IN JOB DEFINITION AND RESOURCING	19
	ISP 3.2 – SECURITY USER TRAINING	
	ISP 3.3 – RESPONDING TO SECURITY INCIDENTS AND MALFUNCTIONS.	21
ΡF	HYSICAL AND ENVIRONMENTAL SECURITY POLICIES	23
	POLICY DIRECTIVE 4.0 - PHYSICAL AND ENVIRONMENTAL SECURITY	23
	ISP 4.1 – Physical Security Access	
	ISP 4.2 – ENVIRONMENTAL CONTROLS.	
	ISP 4.2 – ENVIRONMENTAL CONTROLS ISP 4.3 – CLEAR SCREEN AND CLEAN DESK	
	OMMUNICATIONS AND OPERATIONS MANAGEMENT POLICIES	
	POLICY DIRECTIVE 5.0 - COMMUNICATIONS AND OPERATIONS MANAGEMENT	
	ISP 5.1 – OPERATIONAL PROCEDURES AND RESPONSIBILITIES	
	ISP 5.2 – SYSTEM PLANNING AND ACCEPTANCE	30



	LTH AND WELLNESS	AHW Information Security Policy Manual	July 2007
ISF	5.3 – PROTECTION	AGAINST MALICIOUS CODE	
ISF	5.4 – Information	N BACKUP AND LOGGING	33
ISF	5.5 – Network M	ANAGEMENT	35
ISF	5.6 – MANAGEMEN	NT OF REMOVABLE COMPUTER MEDIA	36
ISF	5.7 – EXCHANGES	OF INFORMATION AND SOFTWARE	38
ISF	5.8 – Appropriati	E USE OF ELECTRONIC MAIL AND INTERNET	40
AUT	HENTICATION A	AND ACCESS CONTROL SECURITY POLICIES	42
Po	LICY DIRECTIVE 6.0	- AUTHENTICATION AND ACCESS CONTROL	42
		QUIREMENT FOR ACCESS	
ISF	6.2 – USER ACCES	S MANAGEMENT	44
ISF	6.3 – Affiliate Ri	ESPONSIBILITIES	46
ISF	6.4 – Network A	CCESS CONTROL	47
ISF	6.5 – OPERATING S	SYSTEM ACCESS CONTROL	49
ISF	6.6 – APPLICATION	ACCESS CONTROL	50
		SYSTEM ACCESS AND USE	
ISF	6.8 – SECURED REI	MOTE ACCESS DEVICES	53
SYST	TEMS DEVELOP	MENT AND MAINTENANCE SECURITY POLICIES	54
Po	LICY DIRECTIVE 7.0	- SYSTEMS DEVELOPMENT AND MAINTENANCE	54
		EQUIREMENTS OF SYSTEMS	
ISF	7.2 – SECURE DEV	ELOPMENT STANDARD	56
		PHIC CONTROLS	
		System Files	
		ELOPMENT CHANGE CONTROL	
		CCESS	
LEG	ISLATIVE COMP	PLIANCE SECURITY POLICIES	63
Po	ICY DIRECTIVE 8 0	- LEGISLATIVE COMPLIANCE	63
		WITH LEGAL REQUIREMENTS	
		SECURITY POLICY AND TECHNICAL COMPLIANCE	
		ECURITY POLICIES	
		- RISK ASSESSMENT	
		MENT METHODOLOGY	
ISF	9.2 – ORGANIZATIO	ONAL RISK ASSESSMENT	
IV.	DEFINITIONS.		70
V.	REFERENCES.		75
AL.	BERTA HEALTH ANI) WELLNESS REFERENCES	75
		FRTA REFERENCES	

AHW Protected ii



I. Executive Summary

Information Security is a key component of Information Management. The Policy Directives and Information Security Policies contained in this document provide Alberta Health and Wellness Affiliates (ie: employees, agents and contractors) with the guidance needed to protect the Confidentiality, Integrity, and Availability of Alberta Health and Wellness' Information. The Policy Directives referred to in the Information Security Policy Manual are not associated with the directives issued to Regional Health Authorities under the Regional Health Authorites Act, RSA 2000. This document is the Information Security Policy Manual.

The Information Security Policy Manual has been developed to ensure it follows Alberta Health and Wellness' Information Security Principles, which are defined in the Information Security Policy Manual Governance section. The Information Security Policy Manual is in compliance with the Health Information Act, RSA 2000, c. H-5 current as of October 31, 2006 and the Health Information and Protection of Privacy Act, RSA 2000, c. F-25 current as of May 26, 2006. The Information Security Policy Manual documents the security requirements needed to ensure that Information is safeguarded, security events are detected, Incidents are prevented or mitigated, and ensures that all Information is compliant with policy.

II. Information Security Policy Governance

Introduction

Information Security protects the Confidentiality, Integrity, and Availability of Information and includes the Security Management, administrative and technical Security Controls of Information.

The Information Security Policy Manual is a statement of intent and guidance by executive management to the organization as a whole regarding the commitment, ownership, responsibilities, processes, and other themes applicable to Information Security Policy Manual defines the expected behaviours, responsibilities, and rules that are required to be enforced.

Information security is a responsibility shared by Alberta Health and Wellness Affiliates. While this document and the implementation may place specific requirements for compliance for agents and contractors, it is not intended to displace a strong security program in those organizations, but assumes they will implement their own Information Security programs for protecting Information within their control. While Information Security is the responsibility of everyone, the Information Policy and Compliance Unit within the Information Management Branch of the Information Strategic Services Division is responsible for development of the Information Security Policy Manual, and the Information Technology Branch is responsible for implementing the Security Controls required to comply with the Information Security Policy Manual.

Organization of the Information Security Policy Manual

A Policy Directive is a high level statement that provides guidance for the development of specific Information Security Policies. Information Security Policies specify how an Alberta Health and Wellness will distribute, manage and protect Information. The Policy Directives and Information Security Policies contained in the Information Security Policy Manual are organized according to all of the major sections of the ISO/IEC 17799:2000 document; except the "Security Policy" section because the Information Security Policy Manual's Information Security Policy Governance section fulfills this role and the "Business Continuity Management" section because the Alberta Health and Wellness Emergency Health Services Branch is responsible for business continuity. Each of the policy groupings in the Information Security Policy Manual start with an overall Policy Directive and are then followed by a number of associated Information Security Policies. Information Security Standards are stand-alone documents and are referred to in application Information Security Policies.



Goal and Objective

The goal and objective of the Information Security Policy Manual is to protect Information, in compliance with the <u>Health Information Act, RSA 2000, c. H-5</u> current as of October 31, 2006 and the <u>Freedom of Information and Protection of Privacy Act, RSA 2000, c. F-25</u> current as of May 26, 2006, by maintaining the Confidentiality, Integrity, and Availability of all Information within Alberta Health and Wellness.

Information Security Principles

Information Security Principles represent fundamental statements of value, operation, or belief that defines the organization's approach to Information Security. The Information Security Principles help define the Policy Directives. The guiding Information Security Principles for Alberta Health and Wellness are:

- Responsibilities of Information Security are shared among all Alberta Health and Wellness Affiliates:
- AHW Affiliates are committed to protecting the security, Confidentiality, Integrity, and Availability of Information;
- Information Security Policy will incorporate industry standards and best-practices for Security Controls to safeguard Information. This will define a minimum standard that will be used for all Information:
- Individually identifiable Information managed by AHW will be protected;
- AHW will comply with all applicable federal and provincial legislation as appropriate regarding the protection and disclosure of Information, and;
- AHW will educate all AHW Affiliates regarding their security responsibilities through a formal security awareness program.

Definitions and Abbreviations

A definitions section is provided in section four of the Information Security Policy Manual for reference. Generally, all capitalized terms or phrases contained within the Information Security Policy Manual are defined terms and can be found in the definitions section.

There are a number of abbreviations used in this document; these are listed below for reference:

AHW – Alberta Health and Wellness

ISP - Information Security Policy

ISPM - Information Security Policy Manual

FOIP - Freedom of Information and Protection of Privacy Act

HIA - Health Information Act

IM - Information Management

IT – Information Technology

IPC Unit - Information and Policy Compliance Unit

PAO - Personnel Administration Office

CIO - Chief Information Officer

GoA - Government of Alberta

Applicable Groups

The Policy Directives, Information Security Policies and their supporting Information Security Standards apply to all AHW Affiliates. The ISPM is intended to define the security requirements and responsibilities covering the management of the Information and Information Systems within AHW's control.



The ISPM must be endorsed by all AHW executives, senior managers, and managers who in turn are responsible for ensuring all AHW Affiliates understand their responsibilities to protect the Confidentiality, Integrity, and Availability of AHW Information.

Statement of Applicability

The administration of the ISPM is the responsibility of the IPC Unit and the Information Management branch except:

- Physical security of AHW is the responsibility of Corporate Operations Division;
- Records and data taxonomy and disposition are the responsibility of the Corporate Records Management office;
- Business continuity which is the responsibility of the Emergency Health Services Branch in the Program Services Division; and
- Employee procedures and discipline, which is the responsibility of Human Resources.

The implementation of technical Security Controls needed to comply with the ISPM is the responsibility of the Information Technology (IT) Branch of the Information Strategic Services Division.

Non-compliance and Deviations

Deviations to policy may be allowed if consent is received from the AHW Security Officer using the Security Policy Exception Process.

The severity of the circumstances would determine the type and severity of disciplinary actions that might be taken against those responsible for non-compliance with AHW's ISPM. The possible disciplinary actions that could be taken against employees includes: verbal reprimand, written reprimand, suspension (with or without pay), demotion and/or termination.

Alignment

This document, "Information Security Policy Manual" aligns with ISO/IEC 17799:2000. ISO/IEC 17799:2000 is a code of practice for Information Security management and is available from the International Organization for Standardization.

Obligations

The <u>Health Information Act, RSA 2000, c. H-5</u> current as of October 31, 2006, the <u>Freedom of Information and Protection of Privacy Act, RSA 2000, c. F-25</u> current as of May 26, 2006, the <u>Government of Alberta Information Technology Security Policy</u> and the <u>Government of Alberta Information Technology Baseline Security Requirements</u> outline the obligations that AHW must comply with regards to protection of Information. The need for all policies within the ISPM is provided by the Health Information Act, section 60.

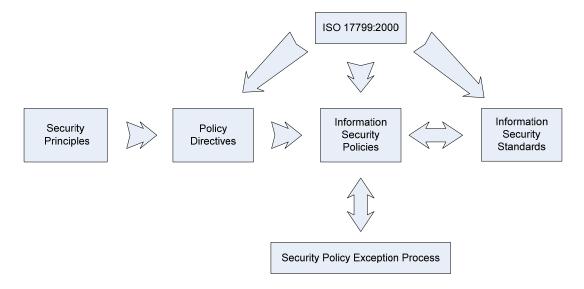
Compliance with Policy

AHW Executives, Senior Managers and Managers are responsible for ensuring that all AHW Affiliates in their business unit comply with AHW's ISPM.



Information Security Development Process

The following diagram demonstrates the developmental process for the ISPM Policy Directives, Information Security Policies and Information Security Standards used within AHW. The ISO/IEC 17799:2000 Code of Practice is an integral component of AHW's Information Security as it provides the basis for all Policy Directives, Information Security Policies and Information Security Standards.



Information Security Standards

The IPC Unit will be responsible for the development of Information Security Standards based on the AHW ISPM. While the ISPM provides high-level direction and is generally implementation neutral, the developed Information Security Standards will provide significant detail on the implementation of an Information Security Policy or group of policies.

Standards will be developed and reviewed by the IPC Unit and the AHW Security Working Group as needed. The approval of Information Security Standards is the responsibility of the AHW Security Officer and the Executive Director for the Information Management Branch.



Roles and Responsibilities

Executive Committee (EC):	This Committee is considered the owner of the ISPM. EC is responsible for approving the Policy Directives, Information Security Policies, and governance section of the ISPM.
Chief Information Officer (CIO):	Designated individual who is responsible for overall Information Security of AHW. The Assistant Deputy Minister of Information Strategic Services fills this role.
Information Policy and Compliance (IPC) Unit:	The unit within AHW responsible for Information Security, privacy, and HIA policy. This unit will perform the Information Security function outlined in Policy Directive 1.0 (Organizational Security).
Manager, Information Compliance and Security (Security Officer):	Responsible for the interpretation of the policies outlined in the ISPM. Is also the head of the AHW Security Working Group, which is an Information Security forum for AHW.
AHW Security Working Group (SWG):	A discussion form that provides support to AHW business units, IT Branch, agents and contractors by focusing on enterprise-wide security issues, planning for resolution, and providing alternative options as appropriate.
AHW Affiliates:	Responsible for abiding by the policies outlined in the ISPM.
AHW Freedom of Information and Protection of Privacy (FOIP) Office	The FOIP Office ensures all supporting policy and administration provides an appropriate balance of access to Information and protection of privacy, in accordance with the intent of the HIA and FOIP Act.

Review Period

The Policy Directives and Information Security Policies contained in the ISPM will be reviewed on an annual basis. Revisions and approvals to each Policy Directive and Information Security Policy will be tracked within the Policy Directive or policy itself.

Review Process

Each Policy Directive or Information Security Policy will be reviewed and approved individually. When a revision, addition or removal of a Policy Directive or Information Security Policy is needed, the review and approval process will be done individually. Before Policy Directives or Information Security Policies are modified, added or removed, analysis must be performed to determine how such changes will impact other areas of the AHW ISPM.

This section, ISPM Governance, will be reviewed and approved independently of the Policy directives and Information Security Policies.

The individual Policy Directives, Information Security Policies and ISPM Governance section must be reviewed by the IPC Unit and the AHW Security Working Group. The approvals for these items are the responsibility of the Security Officer, the Executive Director of the Information Management Branch and ultimately the Assistant Deputy Minister for the Information Strategic Services Division and EC.



July 2007



Information Security Policy Manual Governance Section Version History

The ISPM Governance section has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



III. Information Security Policies

Organizational Security Policies

Policy Directive 1.0 - Organizational Security

Policy Directive:

AHW must maintain an Information Security function to manage Information Security within AHW.

Purpose:

To provide leadership, direction, and governance on policies and standards for Information Security within AHW.

Applicable Groups and Assets:

- All AHW Affiliates
- AHW IT Infrastructure and Non-AHW IT Infrastructure hosted by agents and contractors on behalf of AHW
- AHW Information

Compliance with Policy Directive:

The IPC Unit within the Information Management Branch is responsible for:

- Maintaining the ISPM and assessing the overall security responsibilities of AHW;
- Ensuring the enforcement of the approved ISPM;
- · Reviewing, approving and managing all exceptions to the ISPM;
- Monitoring significant changes in the exposure of Information to major threats:
- Reviewing, monitoring and responding to Incidents as appropriate;
- Reviewing major initiatives to enhance Information Security and;
- Educating AHW Affiliates on the importance of Information Security;
- Conducting and approving Risk Assessments;
- Facilitating external independent reviews of AHW's Information Security practices, and;
- Providing guidance and advice to AHW regarding Information Security matters.

All Third Party contracts must address both physical and logical security concerns. Outsourcing contracts must address Risks and Security Controls.

Alignment:

This Policy Directive aligns with section 4 (Organizational Security) of ISO/IEC 17799:2000.

Versions:

This Policy Directive has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 1.1 - Information Security Infrastructure

Policy Statement:

AHW must have a coordinated security forum with clearly defined responsibilities and roles.

Purpose:

To manage Information Security within AHW to prevent security decisions from being made inconsistently, and to ensure that there is management support for security initiatives.

Applicable Groups and Assets:

- All AHW Affiliates
- AHW IT Infrastructure and Non-AHW IT Infrastructure hosted by agents and contractors on behalf of AHW
- AHW Information

Compliance with Policy:

This AHW internal security forum must be held every 1 to 2 months, with the following responsibilities:

- Reviewing, communicating, and providing feedback on Information Security Policy;
- Reviewing and providing feedback on Risk Assessments;
- Reviewing and monitoring information security Incidents as appropriate;
- Recommending initiatives to enhance Information Security;
- Communicating security topics to different areas within the organization, as well with Third Parties and agents.

This security forum must include representation from:

- Information Management;
- Information Technology;
- · Agents and Contractors;
- Physical Security;
- Business Continuity.

The IPC Unit will chair the AHW internal security forum.

Alianment:

This ISP aligns with section 4.1 (Information Security Infrastructure) of the ISO/IEC 17799:2000 standard. This ISP aligns with Policy Directive 1.0 (Organization Security) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 1.2 - Independent Review of Information Security

Policy Statement:

AHW must have independent reviews performed of its Information Security.

Purpose:

To demonstrate where AHW practices are aligned with the ISPM and provide feedback where AHW practices and policies are not aligned, an independent review must be performed.

Applicable Groups and Assets:

All AHW Divisions, Branches and Units

Compliance with Policy:

An independent review of AHW's Information Security will be conducted every two years. This review must be performed by an external agent. It is the responsibility of the IPC Unit to ensure that this independent review is performed.

Alignment:

This ISP aligns with section 4.1 (Information Security Infrastructure) of the ISO/IEC 17799:2000 standard. This ISP aligns with Policy Directive 1.0 (Organization Security) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location

<u>Versions:</u>
This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 1.3 - Security of Third Party Access

This Information Security Policy is under development.



ISP 1.4 - Outsourcing

Policy Statement:

AHW Outsourcing contracts must address Risks, Security Controls, and procedures for Information Systems.

Purpose:

To maintain the security of Information when the operational responsibility for information processing activities has been Outsourced to another organization.

Applicable Groups and Assets:

- AHW Affiliates
- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

Contracts regarding Outsourcing must address the following items:

- Arrangements to ensure that all parties involved in Outsourcing are aware of their responsibility to comply with the AHW ISPM;
- How the Integrity, Availability, and Confidentiality of AHW's Information is to be maintained and tested;
- AHW's right to audit all activities related to the outsourcing contract;
- Description of Information and Information Technology services being made available;
- Service level agreements, and unacceptable levels of service;
- The establishment of an escalation process for problem resolution; contingency arrangements should also be considered;
- Protection of the Confidentiality, Integrity and Availability of Information when Information is stored, processed, transmitted outside of Canada;
- Responsibilities regarding hardware and software maintenance, installation, and use;
- Arrangements for reporting, notification, and investigation of security Incidents;
- Involvement of the Third Party with sub-contractors;
- All contracts must stipulate the exact uses permitted for AHW's Information held by a contractor or agent and explicitly state that AHW's Information must not be used for any other purpose than those expressly stated in the contract, and;
- All AHW owned Information, systems, documentation, intellectual property; software media (compact disks, floppy disks, etc), software licenses and hardware assets must be dealt with as per the contract at the completion or termination of the contract.

Contractors and agents may need to complete the AHW High Level Security Assessment as required the IPC Unit.

Alignment:

This ISP aligns with section 4.3 (Outsourcing) of the ISO/IEC 17799:2000 standard. This ISP aligns with Policy Directive 1.0 (Organization Security) of the AHW ISPM. This ISP also aligns with section 8(4) of the *Health Information Act* Regulations.



Linked Documents and Items:

Name	Owner	Location
AHW High Level Security	IPC Unit	AHW Security site
Assessment		
Policy for the Protection of Personal	Service Alberta	<u>SHARP</u>
Information in Information Technology		
Outsource Contracts		
Maintaining Security of Government	Service Alberta	Corporate Information
Data Stored on Data Storage Devices		Security site – policy
Policy		<u>section</u>
Contractor's Guide to the FOIP Act	GoA FOIP Office	GoA FOIP Office Site
FOIP Act: A Guide	GoA FOIP Office	GoA FOIP Office site
FOIP Guidelines and Practices	GoA FOIP Office	GoA FOIP Office site

<u>Versions:</u> This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 1.5 - Security Policy Exceptions

Policy Statement:

All deviations from the AHW ISPM must be authorized and managed on an ongoing basis through a well-defined and centralized process.

Purpose:

To manage exceptions through a centralized process so that policies are applied consistently across AHW. Approving and tracking exceptions as needed instead of providing blanket deviations within the ISPM allows AHW to have more control and knowledge over Risks taken.

Applicable Groups and Assets:

- AHW Affiliates
- AHW Information

Compliance with Policy:

The IPC Unit will develop and manage a Security Policy Exception Process to track all policy exceptions.

The Security Officer must approve all exceptions to the AHW ISPM.

Approved Security Policy Exceptions must be reviewed on a regular basis to ensure that conditions of the exception are followed.

Approved Security Policy Exceptions must be temporary with valid start and end dates stated.

Alignment:

This ISP aligns with Policy Directive 1.0 (Organization Security) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
Security Policy Exception Process	IPC Unit	AHW Security site
Security Policy Exception Request	IPC Unit	AHW Security site
Form		

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



Information and Control Policies

Policy Directive 2.0 - Asset Security Classification and Control

This Policy Directive is under development.



ISP 2.1 – Accountability of Information

This Information Security Policy is under development.







ISP 2.2 – Accountability of Business Processes

This Information Security Policy is under development.







ISP 2.3 – Information Security Classification

This Information Security Policy is under development.



Personnel Security Policies

Policy Directive 3.0 - Personnel Security

Policy Directive:

AHW must ensure that the security responsibilities for all AHW Affiliates are clearly defined, documented, communicated, and enforced.

Purpose:

To reduce the Risks of human error, theft, fraud or misuse of Information, all Affiliates must be aware of Information Security threats and concerns, and trained to minimize the damage from security Incidents and malfunctions.

Applicable Groups and Assets:

- All AHW Affiliates
- AHW Human Resources
- AHW Information

Compliance with Policy Directive:

- Personnel security responsibilities must be addressed at the recruitment stage, included in all contracts, and monitored during an individual's employment.
- Potential recruits must go through pre-employment security screening;
- All employees must sign a Confidentiality (non-disclosure) agreement or complete the Government of Alberta Oath of Office;
- All contracts or service agreements must have Confidentiality provisions;
- Affiliates are responsible to report Incidents affecting security to the AHW Help Desk as quickly as possible;
- Affiliates must be trained in security procedures (including security Incident reporting) and the correct use of IT Infrastructure to minimize possible security Risks;
- It is mandatory that all AHW Affiliates participate in security awareness training with periodic refreshers, and;
- Processes must be in place to respond to Provincially Reportable Incidents and internal Incidents.

Alignment:

This Policy Directive aligns with section 6 (Personnel Security) of ISO/IEC 17799:2000.

Versions:

This Policy Directive has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 3.1 - Security in Job Definition and Resourcing

Policy Statement:

AHW security responsibilities must be addressed at the employee recruitment stage, monitored during an individual's employment.

Purpose

To reduce the Risks of human error, theft, fraud, or misuse of Information, security responsibilities must be addressed.

Applicable Groups and Assets:

- All AHW employees
- AHW Human Resources

Compliance with Policy:

Responsibilities for security and Confidentiality of AHW Information must be outlined in employment contracts.

AHW complies with the Government of Alberta Security Screening Directive on which employees must receive a security screening.

Managers will maintain at least monthly contact with employees and periodically review their work to detect potential problems that may lead to a security breach and apply corrective actions as necessary. This requirement must be stated as a common goal in the performance contract for all managers.

The IPC Unit is responsible for maintaining an Information Security Handbook, which must be provided by Human Resources to all AHW employees at commencement of employment.

All AHW employees must take the Government of Alberta Oath of Office.

Alignment:

This ISP aligns with section 6.1 (Security in Job Definition and Resourcing) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 3.0 (Personnel Security) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
GoA Security Screening	PAO	PAO site – Human Resources Directives section
Directive		
GoA Oath of Office	PAO	PAO site
AHW Information Security	IPC Unit	AHW Security site
Handbook		
GoA Information Security	Service	Corporate Information Security Learning Centre
Handbook	Alberta	
GoA Human Resources	PAO	PAO site – Human Resources Directives section
Directives		

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 3.2 - Security User Training

Policy Statement:

All AHW Affiliates must receive security training with periodic refreshers.

Purpose:

To ensure that Information Security is communicated to AHW Affiliates, with periodic reminders, ensuring that the Confidentiality, Integrity, and Availability of AHW Information is maintained by all AHW Affiliates.

Applicable Groups and Assets:

All AHW Affiliates

Compliance with Policy:

All AHW Affiliates must receive Information Security training. This training must include the following points:

- Relevant Information Security Policies and Information Security Standards;
- Updates to the ISPM that would affect the User;
- Security responsibilities of the Affiliate;
- AHW Information Security Handbook;
- Correct and appropriate use of Information Technology assets and Information resources;
- Remote access/Teleworking responsibilities, and;
- Auditing of Affiliates' use of Information Technology assets and Information resources.

All new Affiliates must participate in an Information Security orientation training session within twelve months of starting employment with AHW. Annual refreshers of the training must be offered for Affiliates. Affiliates must attend a security training session refresher once every two years. AHW Human Resources is responsible for tracking Information Security awareness training taken by AHW Affiliates.

Training must be updated on an ongoing basis by the IPC Unit.

Alignment:

This ISP aligns with section 6.2 (User Training) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 3.0 (Personnel Security) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
AHW Information Security Handbook	IPC Unit	AHW Security site
GoA Information Security Handbook	Service Alberta	Corporate Information Security Learning Centre

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3		IPC Unit	AHW SWG, IPC Unit	



ISP 3.3 - Responding to Security Incidents and Malfunctions

Policy Statement:

All Provincially Reportable Incidents and internal AHW security Incidents, security weaknesses, and software malfunctions must be reported.

Purpose:

To mitigate the Risks to Information, Security Incidents or malfunctions must be reported. Reporting will facilitate learning from such Incidents and lower the Risk to Information by limiting the impact to those assets, and providing an opportunity to repair security flaws.

Applicable Groups and Assets:

- All AHW Affiliates
- AHW IT Infrastructure
- AHW Information
- EHR Stakeholders (including Health Authorities, Boards, etc.)

Compliance with Policy:

Internal Incidents

An Internal Incident Response Process must be developed that includes:

- Reporting of Incidents by all employees, agents, and contractors as soon as they become aware of the Incident to a Manager and the IPC Unit, and;
- Reporting of software malfunctions to the help desk, with escalation procedures for Information Security concerns by the help desk to the IPC Unit.

Users must not prove or demonstrate any suspected security vulnerability to AHW's IT Infrastructure. Any suspected security vulnerabilities must be reported to the help desk.

An Incident response process must be developed that includes:

- Post-mortems to review lessons learned, and prevent future Incidents from occurring, and;
- Proper rules for retaining evidence.

Provincially Reportable Incidents

All Provincially Reportable Incidents (Incidents affecting the provincial Electronic Health Record) must be reported as soon as an individual becomes aware of the Incident to the AHW IPC Unit and handled through the Provincially Reportable Incident Response Process.

Alignment:

This ISP aligns with section 6.3 (Responding to Security Incidents and Malfunctions) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 3.0 (Personnel Security) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
AHW Security Policy 8A:	IPC Unit	AHW ISPM
Compliance with Legal Requirements		
Internal Incident Response Process	IPC Unit	21 st Floor Telus Plaza North
(under development)		
Provincially Reportable Incident	IPC Unit	21 st Floor Telus Plaza North
Response Process		
AHW ITIL Incident Management	IT Branch	To be determined
Process		



<u>Versions:</u> This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



Physical and Environmental Security Policies

Policy Directive 4.0 - Physical and Environmental Security

Policy Directive:

AHW requires physical and environment Security Controls to be maintained to protect business premises, IT Infrastructure, and Information.

Purpose:

To prevent the loss, theft, damage or interference of AHW premises, property or Information.

Applicable Groups and Assets:

- AHW IT Infrastructure and Non-AHW IT Infrastructure hosted by agents and contractors on behalf of AHW
- AHW Information
- AHW facilities
- AHW Affiliates

Compliance with Policy Directive:

To mitigate physical security threats, AHW must ensure that Security Controls are in place including:

- Critical or sensitive business information processing facilities must be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry Security Controls;
- Equipment must be physically protected from security threats and environmental hazards.
 Protection of equipment (including that used off-site) is necessary to reduce the Risk of unauthorized access to data and to protect against loss or damage;
- Physical and environmental Security Controls must be maintained by the Corporate Operations Division, and;
- Unattended work areas must be clear of Confidential and Restricted Information.

Alignment:

This Policy Directive aligns with section 7 (Physical and Environmental Security) of ISO/IEC 17799:2000.

Versions:

This Policy Directive has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 4.1 - Physical Security Access

Policy Statement:

Access to AHW Information and sensitive operational facilities and IT Infrastructure must be physically controlled.

Purpose:

To prevent unauthorized access, interference or damage to AHW IT Infrastructure and Information, physical access to AHW Information and sensitive operational facilities and IT Infrastructure must be controlled.

Applicable Groups and Assets:

- AHW IT Infrastructure
- AHW Information
- AHW facilities

Compliance with Policy:

AHW Information and IT Infrastructure must be secured by physical barriers (such as locked doors and walls) and physical security Access Controls, which must comply with the Security Controls outlined in the Information Security Classification Scheme for the level of the asset.

Visitors to secure areas must be authorized for a specific purpose and notified of any security requirement. Visitors should be supervised as necessary.

Alignment:

This ISP aligns with section 7.1 (Secure Areas), 7.2 (Equipment Security), and 7.3 (General Controls) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 4.0 (Physical and Environmental Security) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
AHW Information Security Classification Scheme	IPC Unit	AHW Security site
Policy for Physical Access of Shared RGE Data Facilities	Service Alberta	SHARP
ISP 2.3: Information Security Classification	IPC Unit	AHW ISPM
·		

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 4.2 - Environmental Controls

Policy Statement:

Environmental controls must be in place to reduce the Risk of environmental effects (i.e. fire, smoke, dust, power surges, etc.) on Information and IT Infrastructure.

Purpose:

To protect AHW Information and IT Infrastructure from environmental threats and hazards.

Applicable Groups and Assets:

- AHW IT Infrastructure
- AHW Information
- AHW facilities
- All AHW Affiliates

Compliance with Policy:

Environmental Controls

Environmental controls must be put in place to protect AHW Information according to its security classification and to protect critical IT Infrastructure from environmental threats and hazards. The environmental threats and hazards considered should include fire, smoke, water, electrical supply interference, dust and vibration (this list is not considered to be exhaustive).

Monitoring

Environmental conditions within AHW facilities should be monitored as necessary to allow a prompt response to environmental changes (eg: fire).

Power Controls

Critical Information and IT Infrastructure must have an alternate power supply in case of power failure. Non-critical Information must have Security Controls in place to minimize loss in the event of power failure (e.g. auto-save). Information is deemed critical by a Risk Assessment performed by the IPC Unit.

Eating and Drinking

Eating and drinking will only be permitted at AHW workstations and laptops. Eating and drinking will not be allowed around any other IT Infrastructure or Information.

Alignment:

This ISP aligns with section 7.2 (Equipment Security) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 4.0 (Physical and Environmental Security) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
AHW Information Security Classification Scheme	IPC Unit	AHW Security site

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 4.3 - Clear Screen and Clean Desk

Policy Statement:

Work areas must be protected and clear of any Confidential and Restricted Information when Affiliates are not in contact with them.

Purpose:

To ensure that AHW Information is not subject to compromise when the Information is left unattended.

Applicable Groups and Assets:

- All AHW Affiliates
- AHW Information

Compliance with Policy:

All Confidential and Restricted Information, including files and documents, must be secured at an Affiliate's workstation and work area when left unattended at the end of the business day or when leaving the office.

All workstations and laptops must have a password protected screen timeout of not more than 15 minutes. AHW Affiliates must lock their workstations and laptops when leaving them unattended.

All Confidential and Restricted Information must be cleared from printers and faxes immediately by the recipient or individual printing.

AHW Affiliates who send faxes containing Confidential or Restricted Information must notify the recipient that a fax has been sent.

Alignment:

This ISP aligns with section 7.3 (General Controls) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 4.0 (Physical and Environmental Security) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
AHW Information Security Classification Scheme	IPC Unit	AHW Security site
FOIP Guidelines and Practices	GoA FOIP	GoA FOIP Office site
	Office	

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



Communications and Operations Management Policies

Policy Directive 5.0 - Communications and Operations Management

Policy Directive:

AHW requires that communications and operational Security Controls are implemented to mitigate Risks to Confidentiality, Integrity, and Availability of Information.

Purpose:

To protect the Confidentiality, Integrity, and Availability of AHW Information, operational Security Controls are necessary.

Applicable Groups and Assets:

- AHW IT Infrastructure and Non-AHW IT Infrastructure hosted by agents and contractors on behalf of AHW
- AHW Information
- AHW facilities
- GoA Personnel Administration Office (PAO)

Compliance with Policy:

Operational Security Controls must be implemented including:

- Responsibilities, procedures, guidelines, and documentation for the management and operation of all IT Infrastructure must be maintained by the IT Branch;
- Planning and preparation to ensure the Availability of adequate capacity;
- Implementing Security Controls to detect and prevent the introduction of Malicious Software;
- Maintaining adequate back-up facilities to ensure that all essential business Information and software can be recovered following a disaster or media failure. Back-up facilities are the responsibility of the IT Branch;
- Implementing Security Controls to ensure the security of data in networks, and the protection of connected services from unauthorized access;
- Implementing Security Controls for the management and disposition of removable computer media:
- Controlling and authorizing exchanges of Information and software between organizations and ensuring compliance with any relevant legislation, and;
- The use of electronic mail, and the Internet must be controlled, and have appropriate use guidelines.

Alignment:

This Policy Directive aligns with section 8 (Communications and Operations Management) of the ISO/IEC 17799:2000 Code of Practice.

Versions:

This Policy Directive has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 5.1 - Operational Procedures and Responsibilities

Policy Statement:

Responsibilities and procedures for the management of AHW Information and operation of IT Infrastructure must be established, documented, and communicated.

Purpose

To ensure the correct and secure use of AHW Information and IT Infrastructure through the development and documentation of managerial and operational procedures for AHW Information and IT Infrastructure.

Applicable Groups and Assets:

- AHW IT Infrastructure
- AHW Information
- AHW facilities

Compliance with Policy:

Change Management Process

A formal Change Management process must be developed, documented, implemented and communicated to handle all changes to AHW Electronic Information and IT Infrastructure. This process must be integrated with the systems development change control process and include:

- Assessment of the impact of changes;
- Consultation with the IPC Unit for any change with a Confidentiality, Integrity, or Availability impact:
- A formal approval process for all changes;
- An appropriate escalation process;
- · Documentation of all changes;
- Proper communication mechanism to notify individuals of changes, and:
- Appropriate testing of all changes.

Incident Management Process

A formal Incident Management process must be developed, documented, implemented and communicated for all AHW Information and IT Infrastructure. This process must include:

- A designated owner to ensure documentation is current at all times;
- A communications plan;
- A formal escalation process, and;
- Scenarios to address all potential types of security Incidents (ie: Malicious Software, downtime, hardware failures, etc.).

Configuration Management Process

A formal Configuration Management Process must be developed, documented, communicated, and implemented for all AHW Electronic Information and IT Infrastructure. This process must have a designated owner who will ensure the documentation is current at all times. This process must cover all configurations used within AHW.

Segregation of Duties

If there is a conflict of interest, the operational duties must be segregated. The IT Branch is responsible for reviewing appropriate segregation of duties for its staff every two years.

Release Management

A formal Release Management Process must be developed, documented, implemented, and communicated for all AHW Electronic Information and IT Infrastructure. This process must include:

- A designated owner to ensure documentation is current at all times:
- A communications plan;



- Designated times to rollout patches;
- A formal testing methodology, and;
- Approval from the Change Management process.

Environments

All environments (i.e. testing, development, production) must be logically separated. Security Controls must be consistent between the environments.

Network Infrastructure

Appropriate physical Security Controls must be provided for core network infrastructure. All other exposures of non-core network infrastructure must be minimized. Power cabling and network cabling must be segregated. Sweeps for unauthorized network devices attached to the network must occur on an annual basis. Port access will be controlled as appropriate and all non-AHW equipment requiring port access must be approved through the Security Policy Exception Process.

Maintenance

Information must be maintained by authorized personnel only. All maintenance activities must be recorded, including who did the maintenance, what was performed, and when it was done.

Alignment:

This ISP aligns with section 7.2 (Equipment Security), 7.3 (General Controls), and 8.1 (Operational Procedures and Responsibilities) of ISO/IEC 17799:2000. This policy aligns with Policy Directives 4.0 (Physical and Environmental Security) and 5.0 (Communications and Operations Management) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
AHW ITIL Incident Management	IT Branch	To be determined
Process		
AHW ITIL Change Management	IT Branch	To be determined
Process		
AHW ITIL Configuration Management	IT Branch	To be determined
Process (under development)		
Unauthorized Device Detection	IPC Unit	21 st Floor Telus Plaza North
Process (under development)		
ISP 7.5: System Development	IPC Unit	AHW ISPM
Change Control		
ISP 3.3: Responding to Security	IPC Unit	AHW ISPM
Incidents and Malfunctions		

Versions

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 5.2 - System Planning and Acceptance

Policy Statement:

Advance planning and preparation must be undertaken to ensure that adequate system capacity and resources are available. The operational needs of new Information Systems and upgrades must be defined and tested prior to acceptance and use.

Purpose:

To ensure that AHW IT Infrastructure will continue to have the capacity to meet the needs of AHW Users.

Applicable Groups and Assets:

- AHW IT Infrastructure
- AHW Information
- AHW Users

Compliance with Policy:

Capacity Management

Existing Information Systems must be monitored for capacity (disk space, processor, memory, etc.), and appropriate steps taken to ensure that the capacity is always met. Non-functional requirements for new Information Systems being developed must include capacity requirements.

System Acceptance

Appropriate acceptance criteria must be established for new Information Systems, and upgrades to current Information Systems. This criteria must be clearly defined, and include testing, documentation, performance, capacity requirements, recovery procedures, and training of the new Information System or upgrade.

Alignment:

This ISP aligns with section 8.2 (System Planning and Acceptance) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 5.0 (Communications and Operations Management) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
AHW ITIL Capacity Management	IT Branch	To be determined
Process		

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 5.3 - Protection against Malicious Code

Policy Statement:

AHW Information Systems must be protected against Malicious Software.

Purpose:

To protect the Confidentiality, Integrity, and Availability of Information proper Security Controls must be in place to detect and prevent malicious code in the environment.

Applicable Groups and Assets:

- AHW IT Infrastructure
- AHW Information
- AHW facilities

Compliance with Policy:

Software License

All software must be licensed and authorized through a formal process before use on any AHW Information.

Content Review

Regular reviews of the software and data contents of Information Systems supporting AHW's critical Business Processes will be performed. All unauthorized software and data contents will be removed and investigated as appropriate.

Anti-virus

All files from any source (i.e. floppy disk, CD-ROM, e-mail, etc.) must be scanned by an anti-virus program before being used on AHW Information Systems. Files that cannot be scanned (i.e. password protected ZIP files) must be quarantined. Anti-virus software must be updated at least weekly. All anti-virus patches must be tested before deployment.

Education

Affiliates must be informed that unauthorized software and data contents should not be stored on AHW Information Systems and of the threats posed by malicious code.

Alignment:

This ISP aligns with section 8.3 (Protection against Malicious Software) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 5.0 (Communications and Operations Management) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
ISP 8.1: Compliance with Legal	IPC Unit	AHW ISPM
Requirements		
ISP 3.3: Responding to Security	IPC Unit	AHW ISPM
Incidents and Malfunctions		
ISP 5.1: Operational Procedures and	IPC Unit	AHW ISPM
Responsibilities		



<u>Versions:</u> This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 5.4 - Information Backup and Logging

Policy Statement:

Routine procedures must be established in support of back-up strategies.

Purpose:

To maintain the Integrity and Availability of AHW Information, back-up plans must be a fundamental component in disaster recovery and business continuity plans.

Applicable Groups and Assets:

- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

Back-up

All data must have a back-up that complies with the requirements of the AHW disaster recovery plan, and business continuity plan. Additionally, all back-ups must be tested, stored in a geographically separate location than the data centre, and retained in accordance with applicable records retention policies. The Information Security Classification of the back-up data must meet the same standard as the Production Data.

Back-up Logs

Logs of back-ups and restores must be kept. These Logs must contain the start and completion time of the back-up or restore, any system errors and corrective action taken, what was done with the back-up media, and who conducted the back-up. The IT Branch must review all Logs as needed.

Alignment:

This ISP aligns with section 7.2 (Equipment Security), 7.3 (General Controls), and 8.4 (Housekeeping) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 5.0 (Communications and Operations Management) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
Administrative Records Disposition	GoA Information	GoA Information
Authority	Management Branch	Management site
Transitory Records Retention and	GoA Information	GoA Information
Disposition Schedule	Management Branch	Management site
Developing Records Retention and	GoA Information	GoA Information
Disposition Schedules	Management Branch	Management site
AHW Information Security	IPC Unit	AHW Security site
Classification Scheme		
Backup Log Review Process	IPC Unit	21 st Floor Telus Plaza
(under development)		North
ISP 5.1: Operational Procedures and	IPC Unit	AHW ISPM
Responsibilities		
AHW Business Continuity Plans	AHW Emergency	11 th Floor Telus Plaza
-	Health Services	North
AHW Active Records Retention and	Corporate Records	19 th Floor Telus Plaza
Disposition Schedules	Management Office	North
AHW Information Backup Standard	IPC Unit	21 st Floor Telus Plaza North
V1.0 (under development)		



<u>Versions:</u> This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 5.5 - Network Management

Policy Statement:

The AHW network must have appropriate Security Controls applied.

Purpose:

To maintain the Confidentiality, Integrity, and Availability of the Electronic Information contained on the network, Security Controls must be implemented on the AHW network.

Applicable Groups and Assets:

- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

There must be clearly defined responsibilities for the management of IT equipment within contracts with agents and contractors.

Security Controls must be implemented by the IT Branch to maintain the Confidentiality, Integrity, and Availability of the AHW network, and network services. These Controls must include but are not limited to firewalls, intrusion detection systems, Malicious Software Security Controls, unsolicited mail filtering, patch management, and network segregation.

AHW must comply with the zones of control outlined in the Government of Alberta Enterprise Architecture (GAEA) Security Architecture.

Network vulnerability assessments must be conducted on an annual basis to ensure network Security Controls have not been compromised or misused.

Alignment:

This ISP aligns with section 8.5 (Network Management) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 5.0 (Communications and Operations Management) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
ISP5.1: Operational Procedures and	IPC Unit	AHW ISPM
Responsibilities		
ISP 6.1: Business Requirement for	IPC Unit	AHW ISPM
Access Control		
ISP 5.3: Protection against Malicious	IPC Unit	AHW ISPM
Software		
GAEA Security Architecture version	Service Alberta	SHARP
2.1		
Network Vulnerability Assessment	IPC Unit	21 st Floor Telus Plaza North
Process (under development)		

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 5.6 - Management of Removable Computer Media

Policy Statement:

AHW removable media must be controlled, disposed of securely, and managed.

Purpose:

To maintain the Confidentiality, Integrity, and Availability of the Information stored on removable computer media, AHW removable computer media must have Security Controls in place.

Applicable Groups and Assets:

- All AHW Affiliates
- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

Approval to use removable computer media on AHW computer systems is provided via the AHW Security Policy Exception Process.

Removable computer media must be stored in accordance with the Security Controls listed for the Information Security Classification of the Information on the media. In addition, any special Security Controls by the manufacturer for preserving the media must be complied with.

Removable computer media must be securely disposed of according to the Government of Alberta's Security Policy for Disk Wiping Surplus Computers.

Authorization is required through the Security Policy Exception Process from the IPC Unit before any removable computer media can be removed from an AHW facility.

Alignment:

This ISP aligns with sections 7.2 (Equipment Security), 7.3 (General Controls), and 8.5 (Media Handling and Security) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 5.0 (Communications and Operations Management) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
Government of Alberta Media and File	Service Alberta	Corporate Information
Encryption Standard		Security site – standards
		<u>section</u>
Security Policy for Disk Wiping Surplus	Service Alberta	Corporate Information
Computers		Security site – policy
		<u>section</u>
Maintaining Security of Government Data	Service Alberta	<u>SHARP</u>
Stored on Data Storage Devices Policy		
AHW Information Security Classification	IPC Unit	AHW Security site
Scheme		
AHW Removable Computer Media Standard	IPC Unit	21 st Floor Telus Plaza North
V1.0 (under development)		
ISP 5.4: Information Back-up and Logging	IPC Unit	AHW ISPM
AHW Security Policy Exception Process	IPC Unit	AHW Security site



<u>Versions:</u> This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 5.7 - Exchanges of Information and Software

Policy Statement:

Exchanges of Information between AHW and any external organization must be controlled, compliant with all relevant legislation, and conducted in a secure manner as mandated by the Information Security Classification of the Information.

Purpose:

To prevent loss, unauthorized modification, misuse, or unauthorized destruction of Information exchanged between AHW and any other organization.

Applicable Groups and Assets:

- AHW IT Infrastructure
- AHW Information
- AHW facilities

Compliance with Policy:

All Information exchanged between AHW and an external organization must take into account the Security Controls outlined in the AHW Information Security Classification Scheme.

Formal agreements (ie: Information Manager Agreement) in place for Information and software exchange must include Security Controls appropriate for the sensitivity of the Information being exchanged. These Security Controls must include:

- Management responsibilities for controlling and notifying transmission, despatch and receipt;
- Procedures for notifying sender, transmission, despatch, and receipt;
- Responsibilities and liabilities in the event of loss of data;
- Use of an agreed labelling system for sensitive or critical Information, and;
- Information and software ownership and responsibilities.

Online transactions must follow the Authentication and Authorization Controls outlined in Policy Directive 6.0, ISP 6.1, and ISP 6.2 of the AHW ISPM. A Risk Assessment may be conducted by the IPC Unit as necessary to address the following:

- The level of Authentication needed;
- The level of Authorization needed;
- Auditing requirements;
- Data input validation;
- Vulnerabilities in the office system;
- Identifying those Users who may use the system;
- · Retention and back-up of Information held on the system, and;
- Fallback requirements and arrangements.

Appropriate Security Controls and safeguards must be implemented, and communicated to staff regarding appropriate use of facsimile machines, voice mail, and cellular telephones.

Information Technology assets or Information must not be taken offsite without prior Authorization. Information Technology assets must be tracked when they are removed from site.

Alignment:

This ISP aligns with section 7.2 (Equipment Security), 7.3 (General Controls), and 8.7 (Exchanges of Information and Software) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 5.0 (Communications and Operations Management) of the AHW ISPM.



Linked Documents and Items:

Name	Owner	Location
AHW Information Security	IPC Unit	AHW Security site
Classification Scheme		-
Guide for Developing Personal	GoA FOIP Office	GoA FOIP Office site
Information Sharing Agreements		
FOIP Guidelines and Practices	GoA FOIP Office	GoA FOIP Office site

 $\frac{\text{Versions:}}{\text{This ISP has been revised and approved by:}}$

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 5.8 - Appropriate Use of Electronic Mail and Internet

Policy Statement:

The use of electronic mail, and the Internet must be controlled, and have appropriate use guidelines.

Purpose:

To protect the Sensitive Information exchanged via electronic mail and the Internet and maintain the reputation of AHW.

Applicable Groups and Assets:

- All AHW Affiliates
- AHW Information
- GoA Personnel Administration Office (PAO)

Compliance with Policy:

AHW Affiliates are responsible for ensuring their use of AHW Information Systems does not compromise Sensitive Information or bring disrepute to AHW and does not conflict with their responsibilities as outlined in the laws of Canada, Official Oath of Office Code of Conduct and Ethics for the Public Service of Alberta, and any Supplementary Code of Conduct and Ethics and the terms of their contract, as applicable.

Any Information transmitted across the Internet must not contain personally identifiable Information or health Information unless protected. These types of Information may only be transmitted in a secure manner identified in the AHW Information Security Classification Scheme.

Electronic mail and the Internet may be used for personal use if it does not contain any objectionable material, and does not detract from the performance of the employee.

All electronic mail sent outside of AHW must have the following paragraph of text added to it:

"This e-mail and any files transmitted with it are Confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this e-mail in error please notify the sender of the correspondence. This message contains Confidential Information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail."

Affiliates are responsible for any and all electronic mail sent out with their credentials.

Electronic mail must be retained in accordance to AHW's retention guidelines. Logs of Internet usage and electronic mail must be retained for 3 years.

Potentially hazardous electronic mail attachments (ie: .EXE, .VBS, .SCR, etc.) must not be sent, or received via electronic mail, or downloaded from the Internet. A full listing of unauthorized attachments is maintained by the IT branch.

Alignment:

This ISP aligns with section 8.7.4 (Security of Electronic Mail) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 5.0 (Communications and Operations Management) of the AHW ISPM. This ISP also aligns with the Use of Government of Alberta Internet and E-mail.



Linked Documents and Items:

Name	Owner	Location
AHW Information Security	IPC Unit	AHW Security site
Classification Scheme		
ISP 8.1 :Compliance with Legal	IPC Unit	AHW ISPM
Requirements		
Use of Government of Alberta Internet	Service Alberta	Corporate Information
and Email		Security site - policy section
Policy for the Transmission of	Service Alberta	Corporate Information
Personal Information Via Email and		Security site - policy section
Facsimile		
Managing Instant Messages	Government of Alberta	<u>SHARP</u>
	Information	
	Management	
AHW Secure Electronic Mail Standard	IPC Unit	21 st Floor Telus Plaza North
V1.0 (under development)		
GoA Secure Email Standard	Service Alberta	Corporate Information
		Security site – standards
		<u>section</u>

 $\frac{\text{Versions:}}{\text{This ISP has been revised and approved by:}}$

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



Authentication and Access Control Security Policies

Policy Directive 6.0 - Authentication and Access Control

Policy Directive:

AHW requires that all Information be protected by appropriate and approved Authentication and Access Control mechanisms.

Purpose:

To ensure that Information are not improperly disclosed, modified, deleted, or made unavailable, appropriate Authentication and Access Control must be implemented.

Applicable Groups and Assets:

- AHW Affiliates
- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

To comply with Authorization and Access Control, the following Security Controls must be implemented:

- Access to Information must be justified and approved by a legitimate and clearly defined business need:
- User management must cover all stages in the life-cycle of User access, from the initial registration of new Users to the final de-registration of Users who no longer have a business need to access AHW Information;
- Affiliates must be made aware of and use security best practices regarding Access Control;
- The use of special privileges (i.e. system administrators) must be restricted and controlled;
- User access rights must be reviewed on a periodic basis;
- The level of Authorization to access internal and external network services must follow best practices or be determined by a Risk Assessment;
- Information must have physical and logical Security Controls to restrict access;
- Unauthorized access and inappropriate use of Information and IT Infrastructure must be actively monitored, and;
- Remote access of AHW Information and IT Infrastructure must be secure.

Alignment:

This Policy Directive aligns with section 9 (Authentication and Access Control) of ISO/IEC 17799:2000.

Versions:

This Policy Directive has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 6.1 - Business Requirement for Access

Policy Statement:

Access to Information must have a clearly defined business need and comply with the *Health Information Act* principles of need to know, least amount of Information, and highest degree of anonymity.

Purpose:

To clearly define business requirements to protect the Confidentiality of AHW stakeholders.

Applicable Groups and Assets:

- All AHW Users
- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

Any access to AHW Information must have a clearly defined and documented business need. Access to Information which consists of health Information by AHW Affiliates must receive an Access to Data Holdings (A2DH) approval. Access requests must also take into account the required Security Controls outlined in the AHW Information Security Classification Scheme.

Role based Access Control determined by User roles must be created for common business requirements on an Information System and business unit basis.

Default access to AHW Information must be prohibited. All accesses must be expressly stated and authorized.

Specific Access Control rules must be established for all Information.

Alianment:

This ISP aligns with section 9.1 (Business Requirement for Access Control) of ISO/IEC 17799:2000.

This ISP aligns with Policy Directive 6.0 (Authentication and Access Control) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
Access to Data Holdings Process	IPC Unit	AHW Privacy site
AHW Information Security Classification Scheme	IPC Unit	AHW Security site

Versions

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 6.2 - User Access Management

Policy Statement:

Formal procedures must be implemented to control the allocation of access rights to Information.

Purpose:

To prevent unauthorized access to maintain the Confidentiality, Integrity and Availability of AHW Information.

Applicable Groups and Assets:

- All AHW Users
- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

User Registration

A formal User registration process must be developed, maintained and communicated to ensure that:

- User IDs that are provided are individual specific, auditable, and individually identifiable;
- There is a need to know for the Information, Information is provided in the highest degree of anonymity, and that the least amount of Information is provided;
- The Access to Data Holdings (A2DH) process is followed;
- User IDs are maintained with appropriate access levels, and that redundant User IDs are removed from the system;
- A list of all authorized uses for an Information System must be maintained, and;
- User IDs are audited for access rights and privileges on an annual basis.

Privilege Management

A formal privilege management process must be developed, maintained, and communicated. This process must ensure that:

- User privileges are granted with a need to know, highest degree of anonymity, and that the least amount of Information is granted;
- The Access to Data Holdings (A2DH) process is followed, and;
- User privileges are audited on an annual basis.

User Password Management

A formal password management process must be developed, maintained, and communicated. This process must ensure that:

- Periodic reminders are sent to Users to keep passwords confidential;
- Upon creation of a new User account, a temporary password is provided via a secure method (the use of e-mail is prohibited for providing passwords to Users), and that the password must be changed upon the next login, and;
- User passwords meet the minimum standards outlined in the AHW Password and Timeout Standard. Any Information System password standards that do not meet the AHW Password and Timeout Standard must be authorized by the IPC Unit through the Security Policy Exception Process.

AHW must comply with the Government of Alberta Identity and Authentication Standard.

Review of User Access Rights

User access rights to Information, Information Systems and IT Infrastructure will be reviewed on a periodic basis to ensure only authorized access rights have been granted.



Non-interactive Accounts

All accounts involving no human interaction (non-interactive accounts) are not required to have expiring passwords.

Alignment:
This ISP aligns with section 9.2 (User Access Management) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 6.0 (Authentication and Access Control) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
GoA Shared ICT Infrastructure		SHARP – Policies,
Specifications		Standards, Guidelines
Government of Alberta Identity and	Service Alberta	Corporate Information
Authentication Standard		Security site – standards
		<u>section</u>
Access to Data Holdings Process	IPC Unit	AHW Privacy site
Access to Data Holdings Policy	IPC Unit	AHW Privacy site
AHW Password and Timeout	IPC Unit	AHW Security site
Standard V1.2		
AHW ITIL Change Management	IT Branch	To be determined
Process		
AHW Security Policy Exception	IPC Unit	AHW Security site
Process		
ISP 6.7 – Monitoring System Access	IPC Unit	AHW ISPM
and Use		

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 6.3 - Affiliate Responsibilities

Policy Statement:

All AHW Affiliates must be aware of their responsibilities for practicing appropriate security best practices to maintain Access Control.

Purpose

To prevent unauthorized access by implementing an Access Control system. The cooperation and security awareness of authorized Affiliates is essential to implementing an effective Access Control system.

Applicable Groups and Assets:

All AHW Affiliates

Compliance with Policy:

AHW must educate all Affiliates in good security practices in the selection and use of passwords. This education should include:

- Keeping passwords confidential, and not providing your password to anyone, under any circumstances;
- Avoiding keeping a paper record of passwords, unless it is stored securely at all times, and not stored with the User ID or Information name or Information System name;
- Changing passwords immediately if there is suspected system or password compromise, and:
- Selecting high quality passwords, which do not contain any dictionary words, or names and meet the minimum requirements outlined in the AHW Password and Timeout Standard.

Affiliates must ensure that unattended Information and Information Systems have appropriate security protection. This includes:

- Terminating active sessions when not in use (ie: logging off, or ensuring the screen saver is password protected and working) and at the end of the day, and;
- Physically securing Information when not in use (ie: locking them up).

Alignment:

This ISP aligns with section 9.3 (User Responsibilities) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 6.0 (Authentication and Access Control) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
AHW Password and Timeout	IPC Unit	21 st Floor Telus Plaza North
Standard V1.2		
AHW Information Security Handbook	IPC Unit	AHW Security site

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 6.4 - Network Access Control

Policy Statement:

Network access to AHW Information must be controlled.

Purpose:

To ensure that access to AHW Information is controlled to ensure that the Confidentiality, Integrity, and Availability of Information is not compromised.

Applicable Groups and Assets:

- All AHW Affiliates
- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

Affiliates must only be provided access to AHW Information, Information Systems and IT Infrastructure which they have been specifically authorized to use.

The network path from one subset of AHW Electronic Information to another subset of AHW Electronic Information must be controlled.

Affiliates accessing AHW Electronic Information from an external source must have at least Two-Factor Authentication over a secure channel. Affiliates accessing AHW Electronic Information from an internal source must have at least One-Factor Authentication.

Remote computer systems connecting to AHW Electronic Information must be authenticated.

Access to diagnostic ports on AHW systems must be securely controlled.

AHW Electronic Information must be physically and logically located on the network segment appropriate to the Security Controls outlined in the AHW Information Security Classification Scheme.

Networks which extend beyond AHW boundaries must incorporate User access and routing Security Controls to restrict shared network access.

All services that receive network connections must be documented.

Alignment:

This ISP aligns with section 9.4 (Network Access Control) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 6.0 (Authentication and Access Control) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
ISP 6.1: Business Requirement for	IPC Unit	AHW ISPM
Access Control		
AHW Information Security	IPC Unit	AHW Security site
Classification Scheme		-



<u>Versions:</u> This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 6.5 – Operating System Access Control

Policy Statement:

The ability to modify the operating system must be securely controlled and authorized.

Purpose:

To preserve the Confidentiality, Integrity, and Availability of Information by restricting the ability to modify the operating system.

Applicable Groups and Assets:

- All AHW Affiliates and Users
- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

Only authorized Users are allowed access to AHW Information Systems. In order to restrict unauthorized access, log-on procedures for AHW Information must be developed, which include the following points:

- Information System identifiers must not be displayed until the login process has been successful;
- A general notice warning indicating that the system may only be used by authorized Users must be displayed and acknowledged;
- Help messages (ie: wrong password, or wrong username) must not be provided;
- Log-on input Information must only be validated after all data has been input, and;
- Log-on procedures must be completed within a specified period of time, and be terminated if that time is exceeded.

User IDs assigned to Users must not give any indication to job function, and be unique. The use of a shared User ID is prohibited.

The operating system must have a password management system that can enforce the AHW Password and Timeout Standard.

Access to system utilities must be controlled so that only authorized Users may access them.

Alignment:

This ISP aligns with section 9.5 (Operating System Access Control) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 6.0 (Authentication and Access Control) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
AHW Password and Timeout	IPC Unit	21 st Floor Telus Plaza North
Standard V1.2		
ISP 7.4: Security of System Files	IPC Unit	AHW ISPM

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 6.6 - Application Access Control

Policy Statement:

All AHW Information Systems must have appropriate Access Controls.

Purpose:

To maintain the Confidentiality and Integrity of the Information associated with a given Information System by implementing appropriate Access Controls on a per User basis.

Applicable Groups and Assets:

- All AHW Users
- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

All AHW Information Systems must provide a mechanism for different levels of access based on the AHW Information Security Classification Scheme.

Information systems must not compromise the security of other Information Systems through shared Information output.

The outputs of an Information System must only be sent to authorized Users and the Information sent must be limited to a need to know basis.

AHW Information Systems storing or processing AHW Information with a Restricted Information Security Classification must run on an isolated system.

Alignment:

This ISP aligns with section 9.6 (Application Access Control) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 6.0 (Authentication and Access Control) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
ISP 6.1: Business Requirement for	IPC Unit	AHW ISPM
Access Control		
ISP 6.2: User Access Management	IPC Unit	AHW ISPM
ISP 2.1: Accountability of Assets	IPC Unit	AHW ISPM
AHW Information Security	IPC Unit	AHW Security site
Classification Scheme		

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 6.7 - Monitoring System Access and Use

Policy Statement:

AHW Information and Information Systems must be monitored for unauthorized access and inappropriate use.

Purpose:

To track unauthorized access and misuse of AHW Information and Information Systems by the implementation of logging and other monitoring systems.

Applicable Groups and Assets:

- All AHW Users
- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

All User accesses to Information Systems must be logged for auditing purposes.

All Logs pertaining to Confidential and Restricted Information must be kept both on the individual Information System and a central logging server.

All Logs containing security relevant events must be monitored on an ongoing basis. The level of monitoring must be determined by a Risk Assessment. The results of log monitoring must be reviewed on an ongoing basis.

Logs containing security relevant events must not be reviewed by the individuals whose activities are being reviewed.

All Logs must have Security Controls in place to indicate whether or not the log has been tampered with. These Logs must be kept for three years. In the event that a log has been tampered with or there has been inappropriate access to Information then the log must be kept for 10 years according to Alberta's Limitations Act.

All AHW Information Systems must have their system clocks synchronized against a central time server.

Alignment:

This ISP aligns with section 9.7 (Monitoring System Access and Use) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 6.0 (Authentication and Access Control) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
ISP 8.2: Reviews of Security Policy	IPC Unit	AHW ISPM
and Technical Compliance		
Administrative Records Disposition	GoA Information	GoA Information
Authority	Management Branch	Management site
Transitory Records Retention and	GoA Information	GoA Information
Disposition Schedule	Management Branch	Management site
ISP 6.2 – User Access Management	IPC Unit	AHW ISPM
AHW Audit and Logging Standard	IPC Unit	21 st Telus Plaza North
V1.0 (under development)		



<u>Versions:</u> This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 6.8 – Secured Remote Access Devices

This Information Security Policy is under development.



Systems Development and Maintenance Security Policies

Policy Directive 7.0 - Systems Development and Maintenance

Policy Directive:

AHW requires that appropriate security requirements are identified and agreed upon prior to the development of Information Systems.

Purpose:

To ensure that security is built into IT Infrastructure and Information Systems, including business applications and User-developed applications; security requirements must be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an Information System.

Applicable Groups and Assets:

- AHW IT Infrastructure and Non-AHW IT Infrastructure hosted by agents and contractors on behalf of AHW
- AHW Information
- AHW Information Systems

Compliance with Policy:

The following Security Controls must be implemented:

- All security requirements, including the need for contingency plans, must be identified at the requirements phase of a project and justified, agreed and documented as part of the overall business case for an Information System;
- All Information Systems must comply with a prescribed secure development methodology;
- Activity Logs must be designed into Information Systems and include the validation of input data, internal processing and output data and must be secured;
- Information Systems must undergo testing to ensure security requirements are correctly implemented
- Approved cryptographic services must be used for the protection of Information that have been classified as Restricted or Confidential;
- Access to project and support libraries must be strictly controlled;
- A change control process for the development of Information Systems;
- The use of wireless technology must be controlled;
- All development, testing, and User acceptance testing environments must be physically and logically segregated from production environments, and;
- It is also required that relevant test data be available to perform testing during development of an Information System.

Alianment:

This Policy Directive aligns with section 10 (Systems Development and Maintenance) of ISO/IEC 17799:2000.

Versions:

This Policy Directive has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 7.1 - Security Requirements of Systems

Policy Statement:

All AHW IT Infrastructure and Information Systems must have security requirements defined and documented before development of the Information System.

Purpose:

To ensure that the Confidentiality, Integrity, and Availability concerns of application data are addressed appropriately and timely, Security Controls are incorporated during the design phase of software development.

Applicable Groups and Assets:

- All AHW Users
- AHW IT Infrastructure
- AHW Information Systems
- AHW Information

Compliance with Policy:

Security requirements and Security Controls must be defined and agreed upon before design or implementation of the Information System has occurred. These Security Controls must be based on the Information Security Classification level of the Information associated with the Information System or IT Infrastructure.

Alignment:

This ISP aligns with section 10.1 (Security Requirements of Systems) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 7.0 (Systems Development and Maintenance) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
AHW Information Security Classification Scheme	IPC Unit	AHW Security site

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 7.2 – Secure Development Policy

This Information Security Policy is under development.



ISP 7.3 - Cryptographic Controls

Policy Statement:

AHW Information must have cryptographic controls implemented based on the Information Security Classification of the Information.

Purpose:

To mitigate Risks and provide non-repudiation, the use of cryptographic controls on AHW Information is necessary.

Applicable Groups and Assets:

- All AHW Users
- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

The AHW Cryptographic Standard must be followed for Information classified as Confidential or Restricted under the AHW Information Security Classification Scheme.

All Information classified as Restricted, Confidential or Protected must be encrypted if being transmitted across external uncontrolled networks.

Alignment:

This ISP aligns with section 10.3 (Cryptographic Controls) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 7.0 (Systems Development and Maintenance) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
ISP 8.1: Compliance with Legal	IPC Unit	AHW ISPM
Requirements		
Government of Alberta Cryptographic	Service Alberta	Corporate Information
Standard		Security site – standards
		<u>section</u>
AHW Cryptographic Standard V1.0	IPC Unit	21 st Floor Telus Plaza North
(under development)		
	_	

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 7.4 - Security of System Files

Policy Statement:

Access to system files on AHW Information Systems must be controlled and only granted to authorized users.

Purpose:

To control access to system files on AHW Information Systems to ensure that the Integrity of the system files is maintained, and that the Confidentiality of the asset is maintained.

Applicable Groups and Assets:

- All AHW Affiliates
- AHW IT Infrastructure
- AHW Information
- AHW Information Systems

Compliance with Policy:

All AHW source code must be classified at the same level or higher of Information Security Classification of the production system.

Anonymized Data must be used for testing purposes. Where Anonymized Data is not deemed sufficient for testing purposes, the rationale for requiring the use of Production Data is to be documented and forwarded to the IPC Unit for consideration. The Security Policy Exception Process must be followed for the use of Production Data in testing.

When the use of Production Data for testing purposes is not supported and no other alternative solution exists, the issue will be forwarded to the Assistant Deputy Minister of Information Strategic Services Division for final review and approval.

Test Information must be securely removed from Information Systems immediately after the testing is complete.

Alignment:

This ISP aligns with section 10.4 (Security of System Files) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 7.0 (Systems Development and Maintenance) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
ISP5.1: Operational Procedures and	IPC Unit	AHW ISPM
Responsibilities		
ISP 6.5: Operating System Access	IPC Unit	AHW ISPM
Control		

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 7.5 – System Development Change Control

Policy Statement:

A formal systems development change control process must be implemented for Information and Information Systems that are transitioning from one environment to another.

Purpose:

To maintain the Integrity of AHW Information by ensuring there is a formal change control process.

Applicable Groups and Assets:

- All AHW Users
- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

A formal systems development change control process must be developed, documented, implemented, and communicated for systems development. This process must be integrated with the operational change control process, and address the following:

- Ensure changes are submitted by authorized Users;
- Review controls and Integrity procedures to ensure changes will not compromise system or data Integrity;
- Identify, and track components that require amendment;
- Obtain formal approval for proposals before work commences;
- Ensure that an authorized User accepts the changes;
- Ensure that implementation of the changes minimize business disruption;
- Ensure that system documentation, procedures and User documentation is updated on completion of each change;
- Ensure that a version control document is maintained and updated with each change;
- Ensure that all change requests have an Audit Trail, and;
- Ensure that business continuity and disaster recovery plans are updated with each change.

When any changes occur, appropriate testing procedures must be in place to ensure that the change does not adversely impact the security of the production environment.

Alignment:

This ISP aligns with section 10.5 (Security in Development and Support Processes) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 7.0 (Systems Development and Maintenance) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
ISP 5.1: Operational Procedures and	IPC Unit	AHW ISPM
Responsibilities		
AHW ITIL Change Management	IT Branch	To be determined.
Process		



<u>Versions:</u> This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 7.6 - Wireless Access

Policy Statement:

All access to the AHW IT Infrastructure and Information using wireless technology must be conducted in a secure manner.

Purpose:

To protect the Confidentiality, Integrity and Availability of AHW IT Infrastructure and Information accessed using a wireless technology by preventing unauthorized access and ensuring sustained Availability.

Applicable Groups and Assets:

- AHW IT Infrastructure (including but not limited to Mobile Computing Devices such as laptops, and personal digital assistants)
- AHW Wireless Technology (including IEEE 802.11 technology, Bluetooth, Blackberry, and infrared)
- AHW Information

Compliance with Policy:

Any deployment of wireless technology must follow the AHW Wireless Security Standard and must be reviewed by the IPC Unit. This review must include completion of the AHW Wireless Assessment.

The IPC Unit is responsible for developing, updating, and communicating wireless technology standards.

Information Technology Branch is responsible for ensuring that:

- All requests for any form of wireless access to AHW Information or IT Infrastructure are communicated to the IPC Unit;
- All wireless technologies are implemented correctly according to standards and guidelines, well-managed, available upon demand, and that wireless coverage is the minimum of what is needed;
- Proper physical security countermeasures are in place, and;
- Wireless vulnerability assessments are conducted on a frequent basis, with no more than one year time between them.

Alignment:

This ISP aligns with section 8.5 (Network Management) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 7.0 (Systems Development and Maintenance) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
AHW Wireless Security Assessment	IPC Unit	21 st Floor Telus Plaza North
AHW Wireless Security Standard	IPC Unit	21 st Floor Telus Plaza North
V1.0 (under development)		
Government of Alberta Wireless LAN	Service Alberta	Corporate Information
Access Security Policy		Security site-policy section



<u>Versions:</u> This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



Legislative Compliance Security Policies

Policy Directive 8.0 - Legislative Compliance

Policy Directive:

AHW requires the design, operation, use, and management of AHW Information and IT Infrastructure to comply with statutory, regulatory, and contractual requirements as appropriate.

Purpose:

To ensure AHW Information and IT Infrastructure is compliant with statutory, regulatory, and contractual requirements in order to avoid civil, criminal, or contractual penalties.

Applicable Groups and Assets:

- All AHW Affiliates
- AHW Information
- AHW IT Infrastructure
- AHW Legal and Legislative Services

Compliance with Policy Directive:

The following Security Controls must be implemented:

- Statutory, regulatory, and contractual requirements must be considered for all Information and IT Infrastructure;
- Reviews must be performed to ensure that Information and IT Infrastructure is compliant with the AHW ISPM, and;
- The AHW Chief Information Officer is responsible for the overall security and protection of Information in custody or under control of AHW.

Alignment:

This Policy Directive aligns with section 12 (Legislative Compliance) of ISO/IEC 17799:2000.

Versions:

This Policy Directive has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 8.1 – Compliance with Legal Requirements

Policy Statement:

AHW must comply with all criminal and civil law, statutory, regulatory, or contractual obligations.

Purpose:

To avoid potential penalties by ensuring that Information and IT Infrastructure complies with all applicable legal requirements and contractual obligations.

Applicable Groups and Assets:

- AHW Affiliates
- AHW Information
- AHW IT Infrastructure
- AHW Legal and Legislative Services

Compliance with Policy:

All AHW Information and IT Infrastructure must have all applicable legislation and contractual requirements identified and documented.

All Information needed to comply with applicable legislation requirements and contractual agreements must be kept and protected from loss, destruction and falsification as set out by applicable legislation and contracts.

Alignment:

This ISP aligns with section 12.1 (Compliance with Legal Requirements) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 8.0 (Legislative Compliance) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
Health Information Act, RSA 2000, c.	Government of Alberta	Queen's Printer site
H-5, current as of October 31, 2006		
Freedom of Information and	Government of Alberta	Queen's Printer site
Protection of Privacy Act, RSA 2000,		
c. F-25, current as of May 26, 2006		
Administrative Records Disposition	GoA Information	GoA Information
Authority	Management Branch	Management site
Transitory Records Retention and	GoA Information	GoA Information
Disposition Schedule	Management Branch	Management site
FOIP Guidelines and Practices	GoA FOIP Office	GoA FOIP Office site
Active AHW Records Retention and	Corporate Records	19 th Floor Telus Plaza
Disposition Schedules	Management Office	North

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 8.2 - Reviews of Security Policy and Technical Compliance

Policy Statement:

All AHW Information and IT Infrastructure must have reviews in place to ensure compliance with AHW's ISPM.

Purpose:

To mitigate the Risk of a Confidentiality, Integrity, or Availability breach, reviews of Information and IT Infrastructure are needed to ensure compliance with AHW's ISPM.

Applicable Groups and Assets:

- All AHW Affiliates
- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

Compliance with Security Policy

Periodic reviews must be performed to verify that Information and Business Processes comply with the AHW ISPM and applicable Information Security Standards.

Technical Compliance Reviews

All Information and IT Infrastructure must have reviews in place to ensure that technical implementations are compliant with AHW's ISPM and applicable Information Security Standards.

Alignment:

This ISP aligns with section 12.2 (Reviews of Security Policy and Technical Compliance) of ISO/IEC 17799:2000. This ISP aligns with Policy Directive 8.0 (Legislative Compliance) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.2	April 2003	AIPU	Linda Miller	Todd Heron
1.3	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



Risk Assessment Security Policies

Policy Directive 9.0 - Risk Assessment

Policy Directive:

AHW requires a Risk Assessment methodology be maintained and used to identify the Risks to AHW Information.

Purpose:

To enable AHW to understand the Risk to Information, Risk Assessments are performed to identify which Risks exist and the likelihood of occurrence and potential impact of identified Risks.

Applicable Groups and Assets:

- All AHW Affiliates
- AHW IT Infrastructure and Non-AHW IT Infrastructure hosted by agents and contractors on behalf of AHW
- AHW Information

Compliance with Policy Directive:

The following compliance steps must be implemented for AHW as an organization and its projects:

- A formal Risk Assessment methodology must be used to assess the Risk to Information and its associated Business Processes and IT Infrastructure. Risk Assessment techniques may be applied to the whole organization, or parts of it, and;
- Risk Assessments must be used to determine the Security Controls required to properly secure access to AHW Information.

Alignment:

This Policy Directive aligns with British Standard 7799-2:2002 section 4.

Versions:

This Policy Directive has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 9.1 - Risk Assessment Methodology

Policy Statement:

AHW must have a defined methodology for Risk Assessment of Information.

Purpose:

To ensure that Risks are addressed consistently within AHW; and ensure that the appropriate levels of protection for the Confidentiality, Integrity and Availability of AHW Information are applied.

Applicable Groups and Assets:

- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

AHW must have a comprehensive methodology for Risk Assessment of Information. This methodology must include the following assessments:

- Determine the criticality of business assets, including Information Systems;
- Review the underlying IT services; such as computer installations and associated physical security, personnel security, and emergency preparedness and communications networks; databases; software; hardware; security management; level of security education; policies; and systems development that support the identified critical assets;
- Assess AHW's vulnerability to the threats identified in Appendix B Threat Events, Threat Agents, and Threat Classes of the GoA Threat/Risk Assessment Draft Guide;
- Rank the risks quantitatively and qualitatively;
- Assess the likelihood and impact of internal and external threats, and;
- Identify potential and past events that could impact the Department and its external stakeholders.

The Risk Assessment methodology for Information must also address the following:

- When a Risk Assessment must be carried out;
- The process on how a Risk Assessment must be carried out;
- How long a completed Risk Assessment is valid for;
- Applying appropriate Security Controls to reduce Risk;
- Knowingly, objectively accepting Risks with appropriate authority;
- Avoiding Risks by preventing actions that cause Risks, and;
- Transference of Risk to other parties.

Alignment:

This ISP aligns with Policy Directive 9.0 (Risk Assessment) of the AHW ISPM.

Linked Documents and Items:

Name	Owner	Location
Information Risk Analysis Methodologies	Service Alberta	Corporate Security site
(IRAM) documents		
Fundamental Information Risk	Service Alberta	Corporate Security site
Management (FIRM) documents		
AHW Information Risk Assessment	IPC Unit	21 st Floor Telus Plaza North
Standard V1.0		
GoA Threat/Risk Assessment Draft Guide	Service Alberta	SHARP



<u>Versions:</u> This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



ISP 9.2 - Organizational Risk Assessment

Policy Statement:

AHW must conduct an enterprise wide Risk Assessment.

Purpose:

To ensure that AHW is aware of the threats, vulnerabilities and resulting Risk that it faces as an organization and the Security Controls that could be implemented to mitigate that Risk.

Applicable Groups and Assets:

- All AHW Affiliates
- AHW IT Infrastructure
- AHW Information

Compliance with Policy:

AHW must conduct a comprehensive Risk Assessment on all critical AHW Information and IT Infrastructure annually.

A comprehensive Risk Assessment must be performed for all non-critical AHW Information and IT Infrastructure on a periodic basis.

Alignment:

This ISP aligns with Policy Directive 9.0 (Risk Assessment) of the AHW ISPM.

Linked Documents and Items:

	Name	Owner	Location
AHW Inforr Standard V	nation Risk Assessment 1.0	IPC Unit	21 st Floor Telus Plaza North

Versions:

This ISP has been revised and approved by:

Version	Date	Author	Reviewers	Approval
1.0	July 12, 2007	IPC Unit	AHW SWG, IPC Unit	Executive Committee



IV. Definitions

Access Control: The ability to physically and logically define and restrict who can access resources (data, software, or other resources on the systems), and what level of authority is permitted (read, write, delete, execute).

Affiliate: Refer to the Alberta Health Information Act for the definition of an Affiliate.

Alberta Netcare: The Electronic Health Record for the province of Alberta.

Anonymized Data: Data that has been transformed to protect Sensitive Information from being revealed. The complexity of the transformation applied to particular datasets to anonymize it, is dependent on the other Information and technologies available to the recipient of the Anonymized Data.

Audit: An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.

Audit Trail: Data collected and potentially used to facilitate an Audit.

Authentication: The process established to prove the validity of a claimed identity.

Authorization: The process of giving someone permission to do something.

Availability: The premise that Information is consistently available for authorized Users, entities, or processes when needed to fulfil their business and legal obligations.

Availability Management Process: An Information Technology Infrastructure Library process that optimizes the capability of the IT Infrastructure and supporting organization to deliver a cost effective and sustained level of Availability that enables the business to satisfy its business objectives.

BS 7799-2:2002: This is the British Standards Institute's "Information security management systems – Specification with guidance for use". It documents generally accepted best practices for Information Security and was replaced by **ISO/IEC 17799:2000**.

Business Process: A Business Process is a set of linked activities that create value by transforming an input into a more valuable output. Business Processes are usually supported by Information Systems.

Capacity Management Process: An Information Technology Infrastructure Library process that is responsible for ensuring that IT processing and storage capacity matches the evolving demands of the business in the most cost effective and timely manner.

Change Management Process: An Information Technology Infrastructure Library process of controlling changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved changes with minimum disruption.



Confidential: The AHW Information Security Classification Scheme classification category applied to Information that is sensitive within AHW and could cause serious loss of privacy, competitive advantage, loss of confidence in AHW services, damage to partnerships, relationships and reputation. Confidential Information is available only to a specific function, group or role. Confidential Information includes individually identifiable personal or health Information.

Confidentiality: The premise that Information is not made available or disclosed to unauthorized individuals, entities, or processes.

Configuration Management Process: An Information Technology Infrastructure Library process of identifying and defining configuration items in a system, recording and reporting status of configuration items and request for change, and verifying the completeness and correctness of configuration items.

Custodian: Refer to the Alberta Health Information Act for the definition of Custodian.

Electronic Health Record: A clinical health Information network that links community physicians, pharmacists, hospitals and other authorized health care professionals across the province. It lets these health care professionals view, and in some cases, update key health Information such as a patient's allergies, prescriptions and lab tests.

Electronic Information: Any combinations of data used to support specific business needs that can be transmitted electronically.

Encryption: The cryptographic transformation of Information to render it unintelligible through an algorithmic process using a key.

FOIP: Freedom of Information and Protection of Privacy Act and Regulations.

HIA: Health Information Act and Regulations.

Incident: An actual or suspected case where Information is compromised.

Incident Management Process: The Information Technology Infrastructure Library process that seeks to restore normal service operation as quickly as possible and that minimizes the adverse impact business operations, thus ensuring that the best possible levels of service quality and Availability are maintained.

Information: Combinations of data used to support specific business needs found in both databases and documents.

Information Management: The planning, protecting, organising, classifying, storing, distribution, manipulating, and controlling of Information throughout its life cycle

IPC Unit: The unit within AHW responsible for Information Security, privacy, and HIA policy.

Information Security: The protection of Information resources from accidental or intentional unauthorized collection, access, disclosure, modification, or destruction, or the inability to use that Information.

Information Security Classification: A classification that is given to Information based on its need for Confidentiality, Integrity and Availability.



Information Security Classification Scheme: A system that applies a classification to Information from a defined category on the basis of its sensitivity to disclosure, modification or destruction. The AHW Information Security Classification Scheme classification categories are Restricted, Confidential, Protected and Unrestricted.

Information Security Policy (ISP): A policy statement that specifies how an organization will distribute, manage and protect Information. The policy statement is based on a higher level Policy Directive.

Information Security Policy Manual (ISPM): The set of criteria for the provision of security services based on global rules imposed for all Users. These rules usually rely on a comparison of the sensitivity of the Information being accessed and the possession of corresponding attributes of Users, a group of Users, or entities acting on behalf of Users. A set of management statements that requires all employees, consultants, contractors and business partners to comply with AHW requirements for physical and logical security.

Information Security Standard: Are requirements for compliance for a particular means of executing a security function resulting from an Information Security Policy. The Information Security Standard defines what methods and mechanism will be used to enforce the policy.

Information System: A collection of interrelated components that collect, process, store and output Information needed to complete or assist a particular Business Process.

Information Technology (IT): Applied computer systems - both hardware and software, and often including networking and telecommunications, usually in the context of an organization.

Integrity: The premise that Information has not been altered or destroyed from its intended form, or content, in an unintentional or an unauthorized manner.

International Organization for Standardization (ISO): together with the International Electro technical Commission (IEC) form the specialized system for worldwide standardization.

ISO/IEC 17799:2000: This is the International Organization of Standardization's "Information Technology - Code of Practice for Information Security Management". It documents generally accepted best practices for Information Security.

IT Infrastructure: The sum of an organisation's IT related hardware, networks, software, data telecommunication facilities, procedures and documentation. The IT Infrastructure for a large organization is compromised of many Information Systems.

Life cycle: The course of developmental changes through which information content or an information system passes from initial creation through mature uses to final disposition or replacement.

Logs: Computer records created by systems to track usage, access, errors and other relevant details.

Malicious Software: Software that negatively affects the Integrity of software and Information, examples include computer viruses, network worms, Trojan horses and logic bombs.

Mobile Computing Device: Any communications device that enables staff to work remotely from various locations outside of AHW offices. This includes laptop computers, handheld computers, and cellular phones.

Non-AHW IT Infrastructure: Any IT Infrastructure that is not owned directly by AHW, but is owned by agents and contractors of AHW and is used to provide services to AHW.



One-Factor Authentication: Any User Authentication protocol that requires one method to establish identity and privileges.

Outsourcing: When AH&W contracts to a Third Party for Information processing, Information Systems, networks and/or desktop environment services

Policy Directive: A high level statement that provides guidance for the development of specific Information Security Policies. The Policy Directives referred to in the Information Security Policy Manual are not associated with the directives issued to Regional Health Authorities under the *Regional Health Authorites Act, RSA 2000.*

Production Data: Real data from an operational Information System that may contain individually identifiable Information.

Protected: The AHW Information Security Classification Scheme classification category applied to Information that is sensitive outside of AHW and could impact service levels or performance, or result in low levels of financial loss to individuals or organizations. Protected Information is available to employees, contractors and agents possessing a need to know for business related purposes. Protected Information includes non-identifiable personal or health Information and drafts of documents that will become publicly available.

Provincially Reportable Incident: Any significant breach to the Confidentiality, Integrity, or Availability of any system that is either integral or is a direct input to the provincial EHR.

Record: Information created, received and maintained as evidence by an organization or person in pursuance of legal obligations or in the transaction of business.

Release Management Process: The Information Technology Infrastructure Library process that is responsible for the storage of authorized software, the release of software into the live environment, distribution of software to remote locations, and the implementation of software to bring it into service.

Restricted: The AHW Information Security Classification Scheme classification category applied to Information that is extremely sensitive and could cause extreme damage to the integrity, image or effective service delivery of AHW. Extreme damage includes loss of life, risks to public safety, substantial financial loss, social hardship, and major economic impact. Restricted Information is available only to named individuals or specified roles. Restricted Information includes Authentication and Authorization credentials for example.

Risk: The likelihood or probability that a loss of Information resources or breach of security will occur.

Risk Assessment: The process of identifying and prioritizing risks to the business, which evaluates the criticality of the IT assets, the threats they face, their vulnerabilities, and the business impact of their risks. Once an organization assesses the risks to its business, management should decide to reduce, transfer, avoid, or accept the risks.

Security Controls: The devices or mechanisms that are needed to meet the requirements of an Information Security Policy.

Security Management: The responsibility and actions required, to manage the security environment, including the Information Security Standards and Information Security Policies.



Security Policy Exception Process: This is a process handled by the IPC Unit to allow for the review, rejection or approval and management of deviations from the Information Security Policy Manual.

Sensitive Information: Comprises Information classified as Confidential, Restricted or Protected.

Teleworking: The substitution of telecommunications for any form of work-related travel. Teleworking usually requires securely accessing remote organizational networks.

Third Party: Persons who are not AH&W staff. Third parties include:

- 1) Custodians and Information Managers under HIA
- 2) Hardware and software maintenance and agent support staff
- 3) Cleaning, catering, security guards and other support services
- 4) Volunteers
- 5) Consultants and
- 6) Contractors

Two-Factor Authentication: Any User Authentication protocol that requires two independent ways to establish identity and privileges.

Unrestricted: The AHW Information Security Classification Scheme classification category applied to Information that is created in the normal course of business that is unlikely to cause harm and is publicly available. Unrestricted Information is available to the public, employees, contractors and agents working for AHW. Unrestricted Information includes press releases and job postings for example.

User: An individual with authorized access to Electronic Information. The Authorization may comprise the ability to view/access, add, delete, and/or update Electronic Information.

User ID: A unique personal User identification code used in the Authentication process.



V. References

Alberta Health and Wellness References

AHW Information S	AHW Information Security Standards			
Owner	IPC Unit			
URL or Location	21 st Floor of Telus Plaza North			
Name of Informatio	n Security Standard			
AHW Audit and Log	gging Standard V1.0 (under development)			
AHW Cryptographic	c Standard V1.0 (under development)			
AHW Mobile Comp	uting Security Standard V1.0 (under development)			
AHW Password and	d Timeout Standard V1.2			
AHW Removable C	AHW Removable Computer Media Standard V1.0 (under development)			
AHW Remote Access Control Standard V1.0 (under development)				
AHW Information Risk Assessment Standard V1.0 (under development)				
AHW Secure Development Standard V1.0 (under development)				
AHW Secure Electronic Mail Standard V1.0 (under development)				
AHW Wireless Security Standard V1.0 (under development)				
AHW Information B	ackup Standard V1.0 (under development)			

AHW Information S	AHW Information Security Processes and Resources				
Owner	IPC Unit				
URL or Location	http://intranet.health.gov.ab.ca/Reddot/340.htm				
Name of Process o	r Resource				
AHW Information S	ecurity Handbook				
AHW Wireless Sec	urity Assessment				
AHW High Level Se	ecurity Assessment V3.0				
Information Security	Information Security Classification Scheme				
Internal Incident Response Process (under development)					
Network Vulnerability Assessment Process (under development)					
Provincially Reportable Incident Response Process					
Security Policy Exception Process					
	Security Policy Exception Request Form				
Unauthorized Device	ce Detection Process (under development)				

AHW Privacy Resources			
Owner IPC Unit			
URL or Location http://intranet.health.gov.ab.ca/Reddot/700.htm			
Process Name			
Access to Data Holdings Process Access to Data Holdings Policy			



Other AHW Resources			
Name / Owner	AHW Business Continuity Plans / Emergency Health Services		
URL or Location	RL or Location 11th Floor of Telus Plaza North		
Name / Owner	Business Processes Inventory / To be determined		
URL or Location (document under development)			
Name / Owner Information Inventory / To be determined			
URL or Location (document under development)			



Government of Alberta References

Governr	Government of Alberta Security Policies			
Owner	Service Alberta			
Name	Government of Alberta Wireless LAN Access Security Policy / Service Alberta			
URL	http://www.servicelink.gov.ab.ca/security/content/Policies.cfm			
Name	Government of Alberta Information Technology Baseline Security Requirements			
URL	https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=3078			
Name	Government of Alberta Information Technology Security Policy			
URL	https://www.sharp.gov.ab.ca/secure/DocDisplay.cfm?DocID=3882			
Name	Maintaining Security of Government Data Stored on Data Storage Devices Policy			
URL	http://www.servicelink.gov.ab.ca/security/content/Policies.cfm			
Name	Policy for Physical Access of Shared RGE Data Facilities			
URL	https://www.sharp.gov.ab.ca/secure/docDISPMlay.cfm?DocID=5647			
Name	Policy for the Protection of Personal Information in Information Technology Outsource Contracts			
URL	https://www.sharp.gov.ab.ca/secure/DocDisplay.cfm?DocID=3293			
Name	Security Policy for Disk Wiping Surplus Computers			
URL	http://www.servicelink.gov.ab.ca/security/content/Policies.cfm			
Name	Use of Government of Alberta Internet and Email			
URL	http://www.servicelink.gov.ab.ca/security/content/Policies.cfm			

Government of Alberta Information Security Standards			
Owner	Service Alberta		
URL or Location	http://www.servicelink.gov.ab.ca/security/content/Standards.cfm		
Information Security Standard Name			
GoA Cryptographic Standard GoA Identity and Authentication Standard GoA Media and File Encryption Standard GoA Secure Email Standard			

Government of Alberta Information Security Resources			
Name / Owner	Information Risk Analysis Methodologies (IRAM) documents / Service Alberta		
URL	http://www.servicelink.gov.ab.ca/security/content/ISF_Material.cfm		
Name / Owner	Fundamental Information Risk Management (FIRM) documents / Service Alberta		
URL	http://www.servicelink.gov.ab.ca/security/content/ISF_Material.cfm		
Name / Owner	GAEA Security Architecture version 2.1 / Service Alberta		
URL	https://www.sharp.gov.ab.ca/secure/DocDisplay.cfm?DocID=4124		
Name / Owner	Information Security Classification / GoA IM Branch		
URL	http://www.im.gov.ab.ca/publications/pdf/InfoSecurityClassification.pdf		
Name / Owner	GoA Information Security Handbook / Service Alberta		
URL	http://www.servicelink.gov.ab.ca/security/Content/Learning.cfm		
Name / Owner	GoA Threat/Risk Assessment Draft Guide / Service Alberta		
URL	https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?docID=5266		



Government of Alberta Records Management Resources				
Owner	ner Government of Alberta – Information Management Branch			
URL or Location http://www.im.gov.ab.ca/index.cfm?page=publications/index.html				
Resource Name				
Administrative Records Disposition Authority				
Developing Records Retention and Disposition Schedules				
Managing Instant Messages				
Managing Personal Digital Assistants				
Transitory Records Retention and Disposition Schedule				

Government of Alberta FOIP Office Resources				
Owner	GoA FOIP Office			
Name URL	Contractor's Guide to the FOIP Act http://foip.gov.ab.ca/resources/publications/pdf/ContractorsBrochure.pdf			
Name URL	FOIP Act: A Guide http://foip.gov.ab.ca/resources/publications/pdf/foipguide.pdf			
Name URL	FOIP Guidelines and Practices http://foip.gov.ab.ca/resources/guidelinespractices/index.cfm			
Name URL	Guide for Developing Personal Information Sharing Agreements http://foip.gov.ab.ca/resources/publications/pdf/PerInfoSharingAgreements.pdf			
Name URL	Freedom of Information and Protection of Privacy Act, RSA 2000, c. F-25 http://www.qp.gov.ab.ca/documents/Acts/F25.cfm			

Other Government of Alberta Resources		
Name / Owner URL	GoA Security Screening Directive / PAO http://www.pao.gov.ab.ca/directives/staffing/privacy-impact-assessment.pdf	
Name / Owner URL	GoA Oath of Office / PAO http://www.pao.gov.ab.ca/staff/oath/Official-Oath.pdf	
Name / Owner URL	GoA Human Resources Directives / PAO http://www.pao.gov.ab.ca/Practitioners/?file=directives/titlepage&cf=5	
Name / Owner URL	GoA Shared ICT Infrastructure Specifications / Service Alberta https://www.sharp.gov.ab.ca/secure/docDisplay.cfm?DocID=6247&nh=1	
Name / Owner URL	Health Information Act, RSA 2000, c. H-5 / GoA http://www.qp.gov.ab.ca/documents/Acts/H05.cfm	

External Resources				
Name / Owner	BS 7799-2:2002 / British Standards Institute			
URL or Location	http://www.bsi-global.com/			
Name / Owner	ISO/IEC 17799:2000 / International Organization of Standardization			
URL or Location	http://www.iso.org			

Alberta Health & Wellness Guidance Notes for Access to Data Holdings

Written and maintained by:
Information Policy and Compliance (IPC) Unit
Information Management Branch
Information Strategic Services Division
April 2008

TABLE OF CONTENTS

1	EXECUTIVE SUMMARY	4
2	ALBERTA HEALTH AND WELLNESS PRIVACY COMMITMENT	4
3	HOW DOES A2DH WORK	4
3.1	What is A2DH?	4
3.2	Overview of the A2DH Process	4
3.3	Requestor's Role and Responsibilities	. 6
3.4	Supervisor's Role and Responsibilities	
3.5	A2DH Administrator's role and Responsibilities	. 6
4	A2DH REQUESTS	6
4.1	Overviews	. 6
4.2	Finding the A2DH Site	
4.3	The A2DH Menu	
4.4	The A2DH Request Form Screen	
4.4.1	Overview	
4.4.2	Requestor Requester ID	
4.4.3	Requestor's Relationship with AHW	
4.4.4	Phone Number	8
4.4.5	Job Title	
4.4.6	Supervisor ID.	
4.4.7	Branch	
4.4.8	Other Branch	
4.4.9	Division	
	Other Division	
	Building Location	
	Other Building Location	
	Type of Access	
	Applications	
	Document Name	
4.4.16	Data Holding's	9
	Building Rationale	
	View Document	
4.4.19	Submit	9
4.4.20	Menu	9
4.4.21	Help	9
	Lookup Requester Screen	
4.5.1		10
4.6	Supervisor's Approval	12
4.6.1	Overview	
4.6.2	Supervisor's ID	14
4.6.3	Phone Number	14
4.6.4	Job Title	14
4.6.5	Branch	14
4.6.6	Division	14
4.6.7	Access Termination Date	14
4.6.8	Requestor Status	

4.6.9	Comments	14
4.6.10	Oath	14
4.6.11	View Document	14
4.6.12	Change the Request	15
	Approve	
4.6.14	Reject	15
	Menu	
	Help	
	A2DH Administrator Approval	
4.7.1	Overview	15
5	REVIEW REQUESTS	15
5.1	Overview	16
5.2	To View a Request	16
5.2.1	Overview	16
6	CONTACT US	17
6.1	Overview	17
7	REQUESTS TO ACCESS AHW IDENTIFIABLE DATA BY NON AHW	
		18
7.1	Overview	18
7.2	Access by Vendors	18
7.3	Access by Other Ministries	.18
7.4	Access to NetCare	18

APPENDIX 1: LIST OF A2DH APPLICATION CONTACTS

1 EXECUTIVE SUMMARY

The Access to Data Holdings (A2DH) administrators are responsible for ensuring that access to identifiable information in Alberta Health and Wellness repositories only occurs based the Health *Information Act* principles of highest level of anonymity, least amount of information and need to know.

AHW employees (Requestors) who require access to identifiable information in AHW application databases should consult with the A2DH application contacts (see appendix 1) to determine what access they require prior to submitting a request for access. Supervisors/Managers, when approving a request are responsible for ensuring that the request is accurate and meets the principles of highest degree of anonymity, least amount of information and need to know. Requests that do not meet these criteria will not be approved by the A2DH Administrators. A service request (SR) cannot be initiated without an A2DH approval number.

There are a few situations where access to AHW application databases by third parties is permitted. Examples of these situations are when there is a contract in place with a vendor, a legal agreement with another Ministry or Netcare Access.

2 ALBERTA HEALTH AND WELLNESS PRIVACY COMMITMENT

Alberta's *Health Information Act (HIA)* section 58 requires that when collecting, using or disclosing health information, a custodian must collect, use or disclose only the amount of health information that is essential to enable the custodian or the recipient of the information as the case may be, to carry out the intended purpose. HIA section 60(1)(c) requires a custodian to take reasonable steps to protect against any reasonably anticipated unauthorized access, use, disclosure or modification of the health information or unauthorized access to the health information.

AHW is committed to protecting the privacy of Albertans and the A2DH process assists in ensuring that AHW employees and third parties have access to the least amount of information needed to complete one's duties and that all access is authorized.

3 HOW DOES A2DH WORK

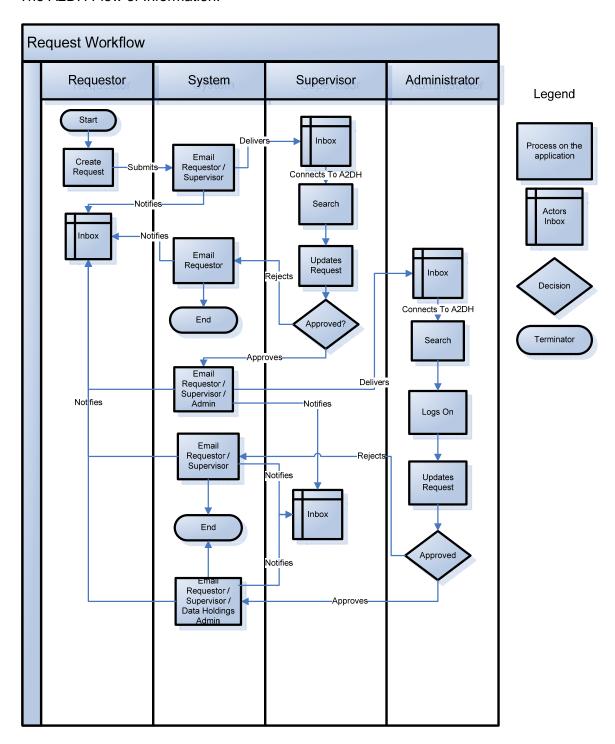
3.1 What Is A2DH?

A2DH is an electronic process that is used to request access to identifiable data in AHW application databases. In order to use the A2DH process, the Requestor must have a valid GOA Requester ID. The A2DH process is a screening process that ensures compliance with HIA. Without an A2DH approval number, a Service Request (SR) cannot be generated to give access to identifiable information in a database. The request for access to identifiable information in AHW application databases must be submitted by a Requestor using the electronic form and then approved by the Requestor's Supervisor. The request is then approved or rejected by the A2DH Administrators.

3.2 Overview of the A2DH Process

The request for access to identifiable information must be created by a Requestor using the electronic form. The Requestor's Supervisor will then review the request and either approve it or reject it. If the request is approved by the Requestor's Supervisor, the request will then be forwarded automatically to the A2DH Administrators for review. The A2DH Administrators will review the request and will either accept the request or reject it. Throughout the A2DH request process, automatic e-mails are sent out notifying people of the progress of the request and action required.

The A2DH Flow of Information:



3.3 Requestor's Role and Responsibilities

The Requestor is responsible for verifying the data that they require access to and for creating the A2DH request. When verifying which data they require access to, the Requestor should discuss this with their supervisor and it is strongly recommended that they consult the A2DH Application Contacts (Appendix 1). There are some databases such as Stakeholder A&A and the Provincial Client Registry, where access will not be granted unless there is written confirmation that the need for access has been reviewed by the database contacts. Access to the BIE should be reviewed with the BI Team in advance to ensure that access to the correct resources/groups are requested. Once the Requester submits the request, the Requester is unable to modify the request.

3.4 Supervisor's Role and Responsibilities

The Supervisor is responsible for reviewing the request and ensuring that it is accurate. If the Supervisor is not satisfied that the access is required in order for the Requestor to perform their duties, then the Supervisor is responsible for rejecting the request. If the request contains inaccurate information, for example, requests access to incorrect tables or the wrong application, then the Supervisor is responsible for changing the request to ensure the accuracy of the information submitted. The Supervisor is then responsible for approving the request.

3.5 A2DH Administrator's Role and Responsibilities

The A2DH Administrator is responsible for reviewing the request. They are unable to make any changes to the content of the request. If there are concerns regarding the request, such as failure to provide confirmation that the application contact has reviewed requests for Stakeholder A&A or Provincial Client Registry, then the request for access will be rejected. When a request is rejected an e-mail is sent to the Requestor and their Supervisor advising of the reasons for rejection. If there are no concerns with the request, then the request for access will be approved and an e-mail will automatically be generated giving the approval number to the Requestor and their Supervisor. This approval number is required for the SR process.

4 A2DH REQUESTS

4.1 Overview

The A2DH process is an electronic process which is accessed through the Alberta health and Wellness Intranet site.

4.2 Finding the A2DH Site

The link to the A2DH site is found on the Alberta Health and Wellness Health Intranet Site on the left side under Global Links. By clicking on the link labeled "Access to Data Holdings", you will be taken to the A2DH site.

4.3 The A2DH Menu

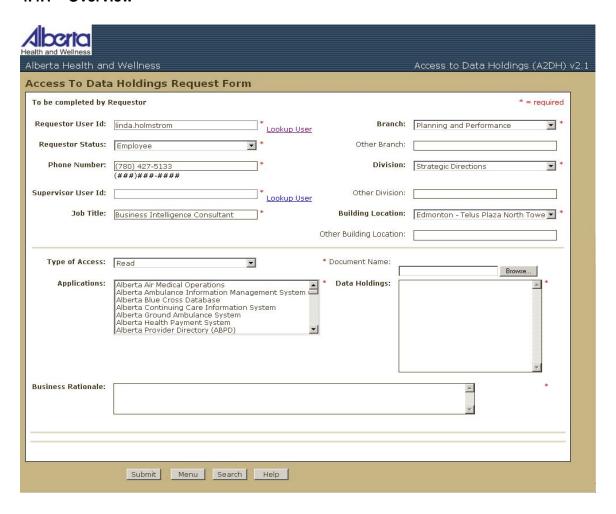
The initial A2DH site is a Menu with three options: Submit Request, Review Requests and Contact Us. Clicking on the Submit Request button will launch the Access to Data Holdings request form (4.3). Clicking on the review request button will launch the Access

to Data Holdings review request screen (5.0). Clicking on the contact us button will take the requester to a new email addressed to the A2DH Administrators (6.0).



4.4 The A2DH Request Form Screen

4.4.1 Overview



The Requestor creates an A2DH request by completing the A2DH Request form. The Requestor must populate the required fields in the Access to Data Holdings form which are marked with a red asterisk. Some of the fields are automatically populated from the "Lookup user" process.

4.4.2 Requestor Requester ID

The Requestor's name must be looked up by clicking on "Look up Requester" (section 4.4). This will take the Requester to the "Look up Requester" Screen.

4.4.3 Requestor's Relationship with AHW

The Requestor must identify their relationship with AHW. These relationships are Appointee, Contractor, Employee, Other, Student and Volunteer. Select the appropriate status by clicking on it.

4.4.4 Phone Number

The phone number needs to be inputted using the GOA standard of 123-456-7890.

4.4.5 Job Title

The Requestor's job title must be inputted.

4.4.6 Supervisor ID

The Supervisor's name must be looked up by clicking on "Look up Requester" (section 4.4). This will take the Requester to the "Look up Requester" Screen.

4.4.7 Branch

The Requestor's branch must be selected from the drop down list by clicking on it. For non AHW GOA employees this drop down list must be populated with "Other".

4.4.8 Other Branch

If there is another Branch that the person works for, this information must be entered.

4.4.9 Division

The Requestor's Division must be selected from the drop down list by clicking on it. For non AHW GOA employees this drop down list must be populated with "Other".

4.4.10 Other Division

If the Requestor is connected to another division, then this must be completed.

4.4.11 Building Location

The default for the building location is TELUS Plaza North Tower. If this is not the correct building location, the Requestor should select the correct building location from the drop

down menu. If the building location is not listed on the drop down list, or if the requester is connected to another building, then "Other" should be selected.

4.4.12 Other Building Location

If the Requester is connected to another building, this information must be entered.

4.4.13 Type of Access

The type of access required will depend on the Requestor's role and duties and will consist of Read, Edit, Create or Remove Access. If Remove Access is selected, then the Supervisor is required to enter a date in the Access Termination Field.

4.4.14 Applications

The Applications are listed in a drop down menu and should be selected. To select multiple applications from the drop down list use the control key.

4.4.15 Document Name

If it is necessary to attach a supporting document, click on Browse and locate the document you wish to attach. After the document is attached to the request it can be reviewed by clicking on the View Document button at the bottom of the page.

4.4.16 Data Holding's

Enter any resources, groups or environments (such as production, BDW, ODS, UAT etc.) that access is required to. If these are in an attachment, reference that attachment.

4.4.17 Business Rationale

The business rationale needs to be completed and will include why the Requestor requires access to this data.

4.4.18 View Document

To view the attached document, click on the "View Document" button.

4.4.19 Submit

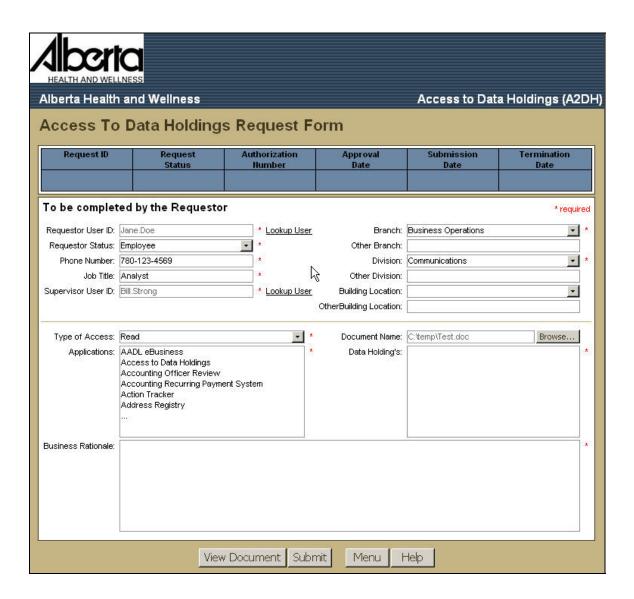
To Submit the Request, click on the "Submit" button. Once the request is submitted the Requestor cannot make any further changes to the request. An e-mail is then automatically sent to the Supervisor advising the Supervisor that there is a request waiting for review and the link to the request is provided. The Requestor is automatically sent a confirmation email.

4.4.20 Menu

The "Menu" button launches the Main A2DH page. Any changes made are not saved in the database.

4.4.21 Help

The "Help" button opens the A2DH Guidelines document.



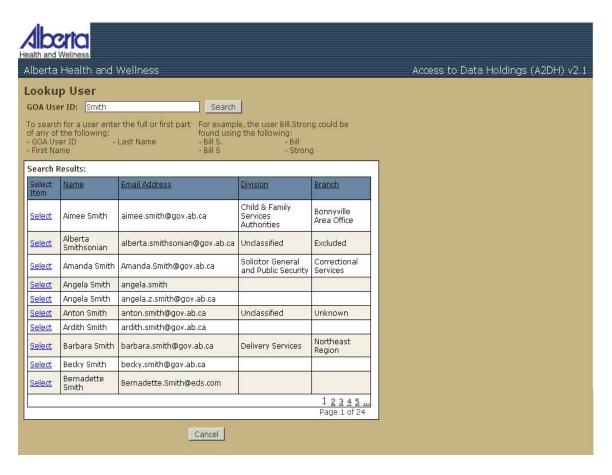
4.5 Lookup Requester Screen

4.5.1 Overview

The Look up Requester screen allows Requestors to search for the requester name using the first name, last name or GOA Requester ID. The Requestor then clicks on "Search" or uses the "Enter" key on the keyboard.



The A2DH system then connects with the GOA directory and will bring up a list of matches. Select the correct match by clicking on it. This will then populate the information in the A2DH Request Form. The same process can be used to populate the Supervisor's information.

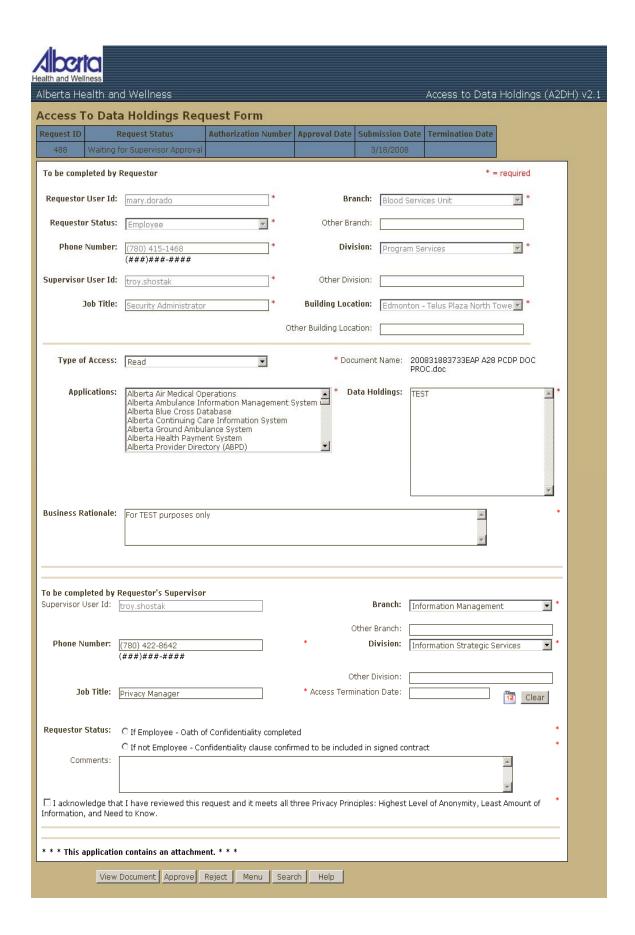


If the "Lookup Requester" search brings up the correct person but incorrect contact information such as an incorrect email address, the supervisor should be contacted to initiate steps in the GOA directory.

4.6 Supervisor's Approval

4.6.1 Overview

The Supervisor receives notification by email that there is an A2DH request waiting for supervisor approval. A link to the request is provided in the email. Only the identified supervisor can open the link and see the A2DH request. The supervisor is responsible for ensuring the accuracy of the information in the request and any attached documents making any changes as required, inputting data in all fields marked with an asterisk and confirming that the request meets the privacy principles of highest level of anonymity, least amount of information and need to know. Some of the fields may be automatically populated by the GOA directory. The Supervisor is also able to make changes to a request.



4.6.2 Supervisor Requester ID

This is automatically populated from the Requestor's request.

4.6.3 Phone Number

The phone number including area code must be in GOA format of 123-456-7890.

4.6.4 Job Title

The Supervisor's job title must be inputted.

4.6.5 Branch

The Supervisor must select their branch from the drop down list. For non AHW GOA employees this drop down list must be populated with "Other".

4.6.6 Division

The Supervisor must select their division from the drop down list. For non AHW GOA employees this drop down list must be populated with "Other".

4.6.7 Access Termination Date

The supervisor inputs the applicable date that the access is to be terminated.

4.6.8 Requestor Status

The supervisor must check one of two boxes. If the Requestor is an employee, then the Supervisor will confirm this and then check the box: "If employee – Oath of Confidentiality completed". If the Requestor is not an employee, then the Supervisor will confirm this and then check the box: "If not employee – confidentiality clause confirmed to be included in signed contract". It is the Supervisor's responsibility to ensure they have confirmed that either an oath of confidentiality is signed or that confidentiality clauses are included in the legal agreement.

4.6.9 Comments

This area is for the Supervisor to make any comments regarding the request that may be helpful in assisting the A2DH Administrators in reviewing the request and approving it.

4.6.10 Oath

At the bottom of the page is an oath that must be reviewed and checked by the supervisor prior to approving the request. The oath states "I acknowledge that I have reviewed this request and it meets all three privacy principles: highest level of anonymity least amount of information and need to know".

4.6.11 View Document

Prior to approving a request for access, the Supervisor must review any attached documents. To review the document, click on the View Document button.

4.6.12 Change the Request

The Supervisor may make changes to the request. Changes can only be made to fields that are not grayed out. Changes to the request will only be saved if the request is approved or rejected. If the screen is closed prior to approval or rejection, the changes will not be saved.

4.6.13 Approve

After the Supervisor has: reviewed the request, made any changes, reviewed any attached documents, determined that access should be granted and completed the oath at the bottom of the page; the Supervisor may approve the request by clicking on the Approve button. If the Supervisor has not completed all required fields, opened any attachments or completed the oath section, the A2DH system will prompt the Supervisor to complete the necessary fields. Once a request is approved, an email is sent to the Requestor, the Supervisor and the A2DH Administrators advising that the request has been approved by the Supervisor and is waiting for A2DH approval.

4.6.14 Reject

If upon reviewing the request and opening any attached documents the Supervisor does not believe that access is required, the Supervisor must reject the request by clicking on the Reject button. When a request is rejected, an email is automatically sent to the Requestor and Supervisor.

4.6.15 Menu

The "Menu" button launches the Main A2DH page. Any changes made are not saved in the database.

4.6.16 Help

The "Help" button opens the A2DH Guidelines document.

4.7 A2DH Administrator Approval

4.7.1 Overview

The A2DH Administrators are responsible for reviewing the request and determining if access should be granted.

The A2DH Administrator may contact the Requestor, Supervisor or A2DH Application Contacts if there are questions regarding the request.

If the request cannot be approved, the A2DH Administrator will notify the Requestor and Supervisor by e-mail that the request is being rejected and why.

If the request is approved, emails are sent to the Requestor, Supervisor, and the A2DH Application Contacts notifying them that the request has been approved and what the approval number is.

5 REVIEW REQUESTS

5.1 Overview

The Review Request screen displays requests that are stored in the electronic A2DH system. The request can be selected by clicking on it and this will bring up the request. Requestors are only able to view their own requests.

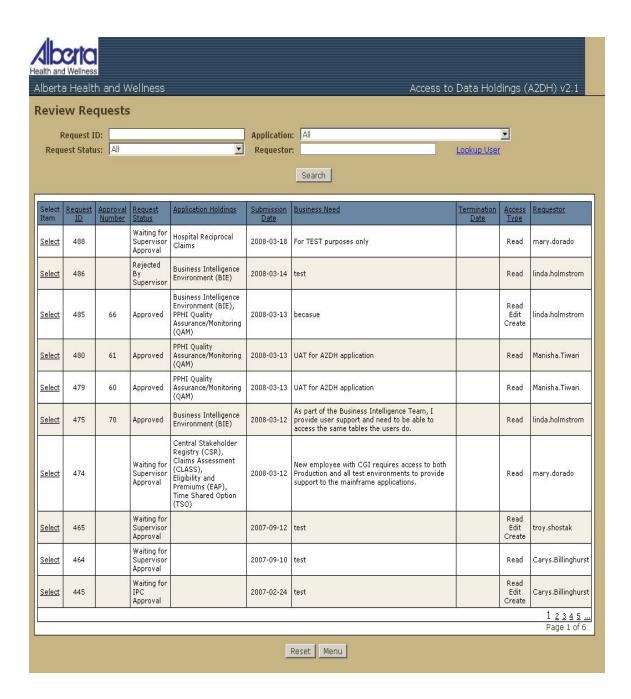
Supervisors are able to view their own requests as well as requests that they have approved.

The A2DH Administrators are able to view all requests in the system.

5.2 To View a Request

5.2.1 Overview

To view a request, click on the Review Requests button and this will launch the Review Requests screen. To select a request, click on it and the request form will be opened.



6 CONTACT US

6.1 Overview

If the "Contact Us" button on the A2DH Main page is clicked, a new email is opened addressed to the A2DH administrators.

7. REQUESTS TO ACCESS AHW IDENTIFIABLE DATA BY NON AHW EMPLOYEES

7.1 Overview

There are a few situations where access to AHW identifiable data by third parties is permitted. Examples of these situations are when there is a contract in place with a vendor, a legal agreement with another Ministry or NetCare Access.

7.2 Access by Vendor Employees

If an employee of a vendor, for example: CGI, Fujitsu or IBM, requires access to AHW identifiable data, the paper version of the A2DH form must be completed. The form must be signed off by a vendor employee's manager. The form is then sent to the identified business (project) contact at AHW.

The identified business contact at AHW is responsible for reviewing the forms and submitting the A2DH request. An A2DH request cannot be submitted until the vendor employee has a valid GOA address. When completing the Electronic A2DH form, the vendor employee is the Requestor and the other business address information would state where the vendor employee was working from and the company name. The Supervisor is the AHW manager from the business area, and they confirm the need for access.

7.3 Access by Other Ministries

If an employee of another Ministry requires access to AHW identifiable information, the paper version of the A2DH form must be completed by the non-AHW employee and signed by their manager. The form is then sent to the business contact at AHW. The AHW business contact is responsible for completing the electronic A2DH form. A manager from the business area is designated as the supervisor who approves the request confirming the need for access.

7.4 Access to NetCare

Custodians cannot access NetCare via A2DH. They must submit a NetCare request to the Privacy Manager, Information Policy and Compliance Unit at AHW.

Appendix 1
List of A2DH Application Contacts

APPLICATION NAME	APPLICATION CONTACT	Business Contact	COMMENTS
Alberta Air Medical Operations	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	NOT YET OPERATIONAL
Alberta Ambulance Information Management System (AAIMS)	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	In A2DH form select e both applications AAIMS and BIE
Alberta Blue Cross Database	Application Contact Not Yet Identified		
Alberta Continuing Care Information System	pauline.michaud@gov.ab .ca	Pauline Michaud	
Alberta Ground Ambulance System			NOT YET OPERATIONAL - Access via Alberta Ambulance Information Management System (AAIMS)
Alberta Health Payment System	Application Contact Not Yet Identified		
Alberta Provider Directory (ABPD)	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	
Alberta Secure Access Service (ASAS)			Decommissioned - No one should be requesting access to it
Alberta Waitlist Registry	darrell.hitchings@gov.ab.	Darrell Hitchings	
Alberta Waitlist Registry	peter.c.marshall@gov.ab. ca	Peter C. Marshall	
Alternate Relationship Plan (ARP)	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	

Automated Micrographic	IRIS ADDUMANUSE CO	Mary Dorado Napov	
Automated Micrographic Image Information System (AMIIS)	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	
Business Intelligence Environment (BIE)	Health.BIEAdministrator @gov.ab.ca	Linda Holmstrom & Manisha Tiwari	
Central Stakeholder Registry (CSR)	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	
Cervical Cancer Screening (CCS)	nancy.hlady@gov.ab.ca	Nancy Hlady	
Claims Assessment (CLASS)	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	
Communicable Disease Reporting System (CDRS) - Notifiable Disease Reporting	rosa.orleski@gov.ab.ca	Rosa Orleski	
Communicable Disease Reporting System (CDRS) - Sexually Transmitted Infections	shirin.ali@gov.ab.ca	Shirin Ali	
Community Health Immunization Information System			Decommissioned - No one should be requesting access to it
Eligibility And Premiums (EAP)	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	
Health Link (H-Link) - Electronic Data Submission	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	
Health Workforce Information Network (HWIN)	Elizabeth.Dufraine@gov. ab.ca	Elizabeth Dufraine	
Home Care Information System			TO BE ACHIVED - No one should be requesting access to it

Home Care Information			TO BE ACHIVED -
System (Local)			No one should be
			requesting access
			to it
Home Care Information			TO BE ACHIVED -
System (Provincial)			No one should be
			requesting access
			to it
Hospital Reciprocal Claims	IBIS.A2DH@gov.ab.ca		
Immunization			TO BE ACHIVED -
			No one should be
			requesting access
			to it
Immunization/Adverse	jill.svenson@gov.ab.ca	Jill Svenson	
Reaction to Immunization (Imm/ARI)			
Integrated Public Health	Glenn.Fraser@gov.ab.ca	Glenn Fraser	
Information System	goriabioa		
(iPHIS)			
Integrated Public Health	myrna.fleischauer@gov.a	Myrna Fleischauer	
Information System	b.ca		
(iPHIS)			
Integrated Public Health	shirley.chorney@gov.ab.	Shirley Chorney	
Information System	ca		
(iPHIS)			
Lab Test Results History	Application Contact Not		
	Yet Identified		
Medical Reciprocal Claims	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy	
		Sandmaier, Laurie	
		Hogan, Maggie	
		Arsenault, Barbara	
		Busse	
Mental Health Patient			TRANSITIONED TO
Advocates Office			CAPITAL HEALTH -
Database			No one should be
			requesting access
Morbidity and	chirley groonen@gov.ch	Shirloy Croopen	to it
Morbidity and Ambulatory Care Abstract	shirley.groenen@gov.ab.	Shirley Groenen	
Reporting (MACAR)	ca		
National Physicians	Application Contact Not		
Database	Yet Identified		
Newborn Metabolic	jill.svenson@gov.ab.ca	Jill Svenson	
Screening (NMS)			
Patient Care Reporting	tyler.james@gov.ab.ca	Tyler James	
System (PCR) (HPPH)			

PD Adapter	Application Contact Not Yet Identified		
Person Directory (PD)	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	
Pharmaceutical Information Network (PIN)			NO ACCESS ALLOWED
PPHI Quality Assurance Monitoring (QAM)	mary.dorado@gov.ab.ca	Mary Dorado	In A2DH form select both applications AAIMS and BIE
PPHI Quality Assurance Monitoring (QAM)	stella.hoeksema@gov.ab. ca	Stella Hoeksema	In A2DH form select both applications AAIMS and BIE
Practitioner Auditing Database	Application Contact Not Yet Identified		
Practitioner Information Retrieval System			TO BE ACHIVED - No one should be requesting access to it
Program Enrolment and Services (PES)	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	
Provincial Client Registry (PCR)	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	NO ACCESS TO BE GRANTED UNLESS APPROVED IN WRITING BY STELLA HOEKSEMA
Provincial Client Registry (PCR) Initiate Hub Auditor	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	NO ACCESS TO BE GRANTED UNLESS APPROVED IN WRITING BY STELLA HOEKSEMA
Provincial Client Registry (PCR) Initiate Viewer	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	NO ACCESS TO BE GRANTED UNLESS APPROVED IN WRITING BY STELLA HOEKSEMA

Provincial Provider Registry (PPR)	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	NOT YET OPERATIONAL
Stakeholder A&A	angie.wong@gov.ab.ca	Angie Wong	NO ACCESS TO BE GRANTED UNLESS APRROVED IN WRITING BY ANGIE WONG
Third Party Liability (TPL)			Should not request TPL, as it is a part of CLASS.
Time Shared Option (TSO)	IBIS.A2DH@gov.ab.ca	Mary Dorado, Nancy Sandmaier, Laurie Hogan, Maggie Arsenault, Barbara Busse	
Tuberculosis Services Registry System			TO BE ACHIVED - No one should be requesting access to it

Branch Contacts for SR Processing						
Branch	Contacts	Comments				
Finance	Dennis Goldsack	Copy both of them.				
	Sherry Mierau					
Client Services	Lorraine Hosack	Copy both of them				
	Betty Penner					
Innovation and Policy	Debra McIntosh					
Alternate Relationships	Ellen Rowsell					
Public Health Policy		The requestor needs to be copied on				
_		the A2DH authorization.				



Alberta Health and Wellness Information Security Handbook



Effective Date: First Revision Date: Second Revision Date: Third Revision Date: Fourth Revision Date: Fifth Revision Date: Approved by: April 1, 2003 September 4, 2003 September 16, 2003 February 3, 2005 June 24, 2005 February 22, 2007 Manager, Information Security and Compliance (780) 427 8089



Table of Contents	1. INTRODUCTION	2
	2. CONFIDENTIALITY AND THE PROTECTION OF	
	INFORMATION	2
	3. HIA AND FOIP	2
	3.1 HIA	_
	3.2 FOIP	
	4. YOUR ROLE	3
	4.1 When You Are Hired or Contracted	9
	4.2 Your Information Security Education	
	4.3 While you work with AHW	
	4.4 When Your Staff/Contractors Leave	
	5. CHIEF INFORMATION OFFICER	4
	6. INFORMATION SECURITY CLASSIFICATION	4
	7. REPORTING SECURITY AND PRIVACY BREACHES	-
	8. PHYSICAL SECURITY	5
	8.1 Zones of Control	
	8.2 Unauthorized persons 8.3 Workspace	
	8.4 Disposal of Records	
	9. COMPUTER AND NETWORK SECURITY	6
	9.1 Responsible Computing	U
	9.1.1 E-Mail Usage	6
	9.1.2 Internet Usage	7
	9.1.3 Adding, modifying, or deleting software and hardware	7
	9.1.4 Personal use of AHW system and equipment	7
	9.2 Passwords	•
	9.2.1 Password Management	8
	9.2.2 Password Construction	8
	9.3 Virus Protection and Detection	
	9.4 How to Secure Your Workstation	
	9.4.1 During the Workday	9
	9.4.2 When Leaving Work	10
	9.5 How to Secure Mobile Computing Equipment	
	10. KEY CONTACTS	11
	10.1 Security	
	10.2 Privacy	
	10.3 All Media	
	10.4 Physical Security	
	11. ONLINE RESOURCES	12
	12. GLOSSARY	13

1. Introduction



Information security is the collection of policies, standards, procedures, and technical and physical controls that protect an organization's information. Information includes electronic systems, databases, hardware, electronic, and physical information. Information security is everyone's job and we all have a role to play. This handbook is a guide to help you follow Alberta Health and Wellness' (AHW) specific information security requirements, in turn reducing the risks associated with misuse of AHW information assets and equipment. It provides a summary of the AHW Information Security Policy Manual.

The Department of Alberta Health and Wellness Minister, Deputy Minister, and all Executives are committed to protecting the confidentiality, integrity, and availability of information. AHW Executive supports the concept that security is a responsibility shared by all affiliates at AHW.

2. Confidentiality and the Protection of Information

We should all be familiar with the concept of confidentiality. In Alberta, the <u>Government Organization Act</u> provides the basis for the confidentiality of provincial government information. Many other pieces of legislation include clauses on confidentiality. For example, the <u>Public Service Act</u> contains the Oath of Office and the <u>Public Health Act</u> protects the confidentiality of communicable disease information.

3. HIA and FOIP

The <u>Health Information Act</u> and the <u>Freedom of Information and Protection of Privacy Act</u> place specific requirements on AHW regarding the protection of health information and personal information. The next two sections explain these requirements in more detail.

3.1 HIA

Under section 1(1) of the *Health Information Act (HIA)*, the Department of Health and Wellness is listed as a "custodian". Custodians are also responsible for ensuring that the health information is protected, collected, used, and disclosed appropriately. Custodians generally have affiliates that include employees or those who perform a service for a custodian as an appointee, volunteer, student or otherwise under a contract or agency relationship. **You are an affiliate of AHW.**

Custodians and affiliates have duties and obligations under *HIA*. Section 60 of *HIA* states that a custodian must take reasonable steps to maintain administrative, technical and physical safeguards that will protect the confidentiality of health information. Section 62 of *HIA* requires all affiliates to comply with the *HIA*, any regulations made under *HIA*, and with any policies and procedures established or adopted under *HIA*.

Section 8(6) of <u>HIA Regulation (70/2001)</u> states that "a custodian must ensure that its affiliates are aware of and adhere to all of the custodian's administrative, technical and physical safeguards in respect of health information." Along with training, this handbook has been provided to you to fulfill this requirement.

3.2 FOIP



The <u>Freedom of Information and Protection of Privacy Act</u> (FOIP) also applies to AHW. AHW and its affiliates must protect all recorded information, including personal information. Section 38 states that "The head of a public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction." Along with training, this handbook has been provided to you to fulfill this requirement.

4. Your Role

4.1 When You Are Hired or Contracted

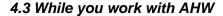
Your security responsibilities begin on the day you are hired or contracted begin. As an affiliate, you must sign the Oath of Office. As a contractor, you must sign a legal agreement that includes clauses of confidentiality (non-disclosure) and compliance with both the <u>Freedom of Information and Protection of Privacy</u> and <u>Health Information Act</u>.

Appropriate management approvals must be provided with respect to your computer logon user IDs and your AHW identification or building access equipment (ie: ID Access badges or keys).

4.2 Your Information Security Education

The AHW Information Security Policy Manual requires that all affiliates receive information security training with periodic refreshers. Your information security training starts with an orientation session that addresses the following:

- Relevant AHW Information Security Policies and Information Security Standards;
- Security responsibilities of an affiliate;
- The AHW Information Security Handbook;
- Correct and appropriate use of information technology assets and information resources;
- Remote access and teleworking responsibilities, and;
- Auditing of affiliates' use of information technology assets and information resources.



You must follow and comply with the AHW Information Security Policy Manual and the information presented in this handbook. The AHW Information Security Policy Manual is available from the Information Policy and Compliance (IPC) Unit.

The IPC Unit investigates all privacy and security incidents. The IPC Unit works to resolve all incidents in non-punitive manner; however, disciplinary action is possible up to and including dismissal.



4.4 When Your Staff/Contractors Leave



Ensure that a Service Request (SR) is submitted several days in advance of your individual staff member's departure date to ensure that computer logon user IDs are inactivated at the end of the individual's workday. On your staff member's or contractor's last day of work with AHW, you must collect that person's identification and building access equipment (ie: ID Access badges or keys) and return them to your supervisor. Security system passwords/codes and cipher lock combinations must be changed at the end of the departing staff member's last day at work. AHW assets such as laptops, PDA's, etc. must be returned before leaving. Follow the Contractor Termination Checklist and the Human Resources Termination Checklist as applicable.

5. Chief Information Officer

The Chief Information Officer is the person who makes decisions on security risk and accepts liability on behalf of AHW. The Chief Information Officer (CIO) is a function provided by the Assistant Deputy Minister (ADM), Information Strategic Services. On a day-to-day working basis the Manager, Information Security and Compliance has the role of assessing risks on behalf of AHW. The Senior Records Officer (SRO) has been delegated responsibility from the Deputy Minister (DM) when dealing with the management of recorded information.

Responsibilities are arranged in order to segregate duties between security management and operation. Managers must ensure that, to the extent possible, no individual has sufficient capability to circumvent key systems controls.

6. Information Security Classification

Information stewards assign classification levels to the respective data, and information holdings they manage based on the AHW Information Security Classification Scheme. AHW affiliates are then required, in accordance with the Information Security Policy Manual, to uphold and adhere to the safeguards and controls ascribed by the classification levels for the information they view, collect, manipulate, store, and process. AHW has four information security classification levels:



- Restricted classification applies to information that would be damaging to the integrity, image, or effective operation of AHW if improperly used or disclosed. Access is very limited.
- Confidential classification applies to information that must be protected from unauthorized disclosure or modification. Access is specific to a job function, group, or role. Generally individually identifying health information and personal information fall under this category.
- **Protected classification** applies to information that is of interest to AHW and must be protected from unauthorized access. Access is available to individuals possessing an authenticated identity.
- *Unrestricted classification* applies to information that has no security access requirements.

The AHW Information Security Policy Manual requires that all information be classified according to the AHW Information Security Classification Scheme.



The definition of the differing levels of security sensitivity and the corresponding responsibilities and management processes are essential to constructing an effective security architecture and management process. The alignment of classifications between AHW program teams and external stakeholders is also required to provide consistent treatment of information flowing between them. Other considerations include:

- The security classification of the information is a fundamental way of understanding the different security requirements of the information and defining how to handle those differences;
- Information generated and maintained within AHW has varying degrees of security requirements depending on the nature and the use of the data;
- All information must be classified by its nature and purpose in order to be able to determine what security processes are required for protection and disclosure of the data;
- An information classification system must define the appropriate set of protection levels, and communicate the need for special handling measures, and:
- The classification of information may change over time. Information deemed at a confidential level now, may drop to an internal level in the future.

Your role in information security classification is to ensure that all information resources are classified, and to protect information resources according to their classification level.

7. Reporting Security and Privacy Breaches



If you experience a computer based security incident, breach, threat, weakness, or malfunction (ie: computer viruses, equipment theft), report it immediately to the **AHW Help Desk at (780) 917 4141**. You must not, under any circumstances, attempt to investigate a suspected weakness or vulnerability yourself. This is for your own protection, as your conduct may cause further damage or be interpreted as potential misuse of the system. Inform the **IPC Unit at (780) 427 8089** if you suspect a weakness.

If any other information security or privacy incidents arise that you wish to discuss, call the AHW Manager, Information Security and Compliance at (780) 427 8089.

For **personal and physical security, contact (780) 4271465** in the case of stolen items and **Building Security at (780) 408 1920** in case of intruders.

8. Physical Security

8.1 Zones of Control

There are different Physical Security Zones of Control in AHW buildings. Physical Security Zones of Control include:

Public Access Zone where the public can freely enter and exit

Internal Access Zone where access is restricted to AHW

All areas of the buildings that the public are encouraged to enter, (ie: front reception areas and libraries) are considered Public Access Zones. Office





areas to which the public is restricted are considered Internal Zones.

When entering by way of a locked door, ensure you are not being closely followed (tailgated). If building doors are closed, leave them closed. Do not prop them open for convenience as it defeats security controls.

8.2 Unauthorized persons

Ensure that AHW personnel escort your visitors at all times. All staff should have an ID badge. If it is not visible, ask to see it. If you see someone without an escort or a visible ID access card, ask to see the ID access card and about his/her business on that floor. If the person refuses to answer, call building security. If you observe or suspect any physical security incidents, e.g., thefts or suspicious behaviour from a member of the public, notify building security at TELUS Plaza North Tower, call: (780) 408 1920

8.3 Workspace

Do not leave any Restricted or Confidential information on your desk overnight or over the weekend; it must be secured in a locked drawer or cabinet. Do not fax any Restricted information at any time.

8.4 Disposal of Records

For transitory records, AHW follows the Government of Alberta's <u>Transitory Records Retention and Disposition Schedule</u>. For retention and disposition of administrative records, AHW follows the <u>Administrative Records Disposition Authority</u>. Affiliates can also refer to the following document for more information: <u>Official and Transitory Records: A Guide for Government of Alberta Employees</u>. Contact the AHW **Senior Records Officer at (780) 415 2786** to discuss the disposal and/or archiving process.

9. Computer and Network Security

9.1 Responsible Computing

Documents must be saved only in your 'My Documents' folder or on the 'M' (shared) drive. On the PC, do not store your data directly on the 'C' Drive as:

- They are not backed up and data can easily be lost
- They may be accessible to an unauthorized person if he/she logs on to your PC
- Due to portability and fragility of computers, there is a high risk of theft or damage and loss or unauthorised access of information

The use of **all** removable computer media (CDs, diskettes, DVDs, USB devices) must be authorized by the Information Policy and Compliance Unit. AHW requires that removable computer media be securely disposed of according to the Government of Alberta's <u>Security Policy for Disk Wiping Surplus Computers</u>. Please refer to section 9.5 for information on how to secure mobile computing equipment.

9.1.1 E-Mail Usage

Do not open any e-mail attachments from a person you do not know. Attachments with extensions such as .vbs, .exe, .com can contain viruses or





worms. Please see section <u>9.3 Virus Protection and Detection</u> for more information on viruses. If you are sending any documents containing Restricted or Confidential information through e-mail via the Internet, the documents must be encrypted contact the **Help Desk at (780) 917 4141** for assistance.

9.1.2 Internet Usage

Your Internet usage is automatically logged and information gathered on you includes: user ID, website locations, length of time at website(s). Supervisors can request this information at anytime.

You must not access or distribute offensive materials. Offensive materials include, but are not limited to, pornography, hate literature, obscene materials, materials which contravene human rights legislation, and any other material that could reasonably be interpreted as a form of sexual or workplace harassment.

You must not undertake activities that are inappropriate, offensive or illegal which include:

- Cyber stalking and/or harassment;
- Defamation and/or libel, and;
- Gambling.

Please refer to the <u>Use of Government of Alberta Internet and Email</u> policy for more information.

9.1.3 Adding, modifying, or deleting software and hardware

You must not alter or install hardware devices or software on AHW computers as it increases the risk of an unstable computer and the potential for viruses (eg: ICQ and MSN web chat site users frequently share files with no virus protection).

You must submit a service request through your work site contact to request the installation of additional software or hardware.

9.1.4 Personal use of AHW systems and equipment

Your use of AHW systems and equipment must not conflict with the Oath of Office, the <u>Code of Conduct & Ethics for the Public Service of Alberta</u> or the <u>Use of Government of Alberta Internet and Email</u> policy. Your personal use of the Internet and e-mail system is permitted provided use is consistent with professional conduct, does not detract from the performance of employment duties, and is not used for personal financial gain. Information systems and business equipment may be used for non-AHW business purposes at the discretion of your supervisor.

9.2 Passwords

When you are assigned a user ID to access any AHW information resource, you are solely responsible for all actions taken while that user ID is in use. Sharing your user ID and/or password with any other person, including associates and assistants, is prohibited.

There are risks associated with sharing your user ID and/or password and allowing associates to automatically access your e-mail. Doing so grants the individual(s) unlimited access to your e-mail where they can also create



and respond to e-mail as you. In addition, they can access your personal and financial information on the GoA My AGent System.

9.2.1 Password Management

The password management function enforces rules for creating and changing passwords. Your responsibility is to:

- Keep passwords confidential;
- Not write down or post your password(s) in view in the desk area;
- Not share your passwords with other staff;
- Change your passwords whenever there is any indication of possible system or password compromise, and;
- Change your temporary password the first time you logon, after it is assigned.

Passwords used less frequently may be written down but must be stored in a locked drawer or cabinet.

Whenever you leave your computer you must lock your workstation. In Windows XP, press "Ctrl - Alt -Del" and select "Lock Computer", or press "Windows key – L", or by clicking the "lock" icon on your Quick Launch Bar.

Of note:

- Passwords will expire after a certain interval and must be reset. A
 process is in place to ensure that a password cannot be re-used until
 after a certain number of intervals. This is a regular IT process and
 you will be notified to change it.
- Passwords must not be included in any automated log on process.
- Users must be authenticated before resetting or assigning any passwords. The Help Desk will authenticate users.
- The security system locks out a user ID after five consecutive failed sign-on attempts.

9.2.2 Password Construction

You must adhere to the AHW Password Standard, which includes:

- Passwords must not contain an individual's user name or full name:
- The minimum number of characters in a valid password is eight.
 This will prevent the use of short names and initials, and;
- Valid passwords must contain three of the following:
 - Upper case letters: A, B, C, ..., Y, Z
 - Lower case letters: a, b, c, ..., y, z
 - Numbers: 0, 1, 2, ..., 8, 9
 - Special characters such as: !, @, #, etc.







9.3 Virus Protection and Detection

A virus is any software that can negatively affect or cause harm to IT systems, data, or networks. There are several forms of virus and methods by which they can cause harm. Viruses that are introduced into any system are at best a nuisance requiring time and effort to deal with them and at worst have the ability to seriously damage or destroy data or systems that will require extensive reconstruction and recovery.

To prevent virus infection and to minimize the impact of viruses encountered, please be aware that:

- Virus scanning tools and software are available and maintained by IT for all corporate desktops and servers. You must not disable any virus prevention and detection software that was implemented and supported by AHW IT;
- Any external data that you introduce into AHW systems must be checked with an approved virus scanning mechanism before being accessed or stored. Contact the AHW Help Desk at (780) 917 4141 to arrange this;
- AHW wide warning and notifications of viruses are the responsibility of the IT Branch, and;
- Notification of the AHW Help Desk at (780) 917 4141 is required if you suspect a virus.

9.4 How to Secure Your Workstation

You must always:

- a) Terminate active computer sessions when finished, unless you have secured your PC by enabling other appropriate locking mechanisms, e.g. power on password, a password protected screen saver, and;
- b) Secure PCs or terminals from unauthorized use by a key lock or an equivalent control, e.g. password access, when not in use.

You should turn the screen away from unauthorized persons (especially in areas where dealing with the public) so that the information is not displayed in the open.

9.4.1 During the Workday

When leaving your workstation for any period of time perform the following steps:

- a) Lock your computer by pressing "Ctrl Alt -Del" and select "Lock Computer", or press "Windows key – L", or by clicking the "lock" icon on your Quick Launch Bar;
- b) Remove any confidential or restricted information and lock it up in a cabinet or drawer, and;
- c) Make sure that there are no passwords or keys left around your workstation.



9.4.2 When Leaving Work

The following steps, if performed correctly will maintain the level of security that AHW requires of its employees:

- a. Remove all restricted, confidential, and protected information and store them in a locked cabinet.
- b. Ensure all cabinets that contain restricted, confidential, or protected information are locked.
- c. Before the weekend or an extended absence, shut down your computer. During the workweek, log off your computer.

Make sure that no passwords or keys are left around your workstation.



Your use of any AHW mobile computing equipment e.g., laptops, Personal Digital Assistants (PDAs), outside of AHW's premises must be authorized by your supervisor.

Do not remove or modify software (e.g. screen savers, anti-virus, network management software) on mobile computing equipment implemented by AHW for any purpose.

Mobile computing equipment must not be loaned to any external parties. Laptops and other portable devices should only be repaired by AHW and not by any third parties. Contact the help desk for your repair needs at (780) 917 4141.

Here are a few guidelines to keep your AHW mobile computing equipment and the information on it secure:

- Does it need to be local? Any files that do not need to be stored locally on the mobile computing equipment should be kept on AHW networks. Only the information required for business needs should be stored on mobile computing equipment.
- 2) Encrypt files If information must remain on your laptop then it must be encrypted. In the case of PDAs any confidential or restricted information on the device must be encrypted. Encryption offers a strong layer of protection from information being accessed if the laptop is lost or stolen. AHW laptops have WinZip 9.0 SR-1 as a standard software package, which has an encryption facility that can be used to protect files. The Information Policy and Compliance Unit developed a document that is available at the <u>AHW Security intranet</u> <u>site</u> to assist people in the use of WinZip 9.0 SR-1 to encrypt files.
- 3) Use a cable lock Most laptops have a security slot that allows a cable lock to be attached. The cable lock will deter opportunistic thieves that would take a laptop that is not secured and slow down more determined thieves. The cable lock should be tethered to a strong object. If your laptop does not have a cable lock, please call (780) 917 4141.







- 4) Locked storage If the mobile computing equipment is not in use and locked storage is available, such as a filing cabinet, then store it in the secure storage area.
- 5) Leaving mobile computing equipment in vehicles Thefts from vehicles is very prevalent. If possible, mobile computing equipment should not be left in vehicles. However, if it is necessary to store the equipment in a vehicle, put the equipment in the trunk out of view and in the case of a laptop use a cable lock to physically secure the laptop to the car if possible. It is very important that the equipment be out of view. It is also recommended that the vehicle have an active alarm system.
- 6) Hotels and airports These are also prevalent locations for laptop thefts from business travellers. If you need to leave your laptop in your hotel room, secure it using a cable lock. For PDAs if there is no secure storage available in your hotel room, then keep the PDA on your person. Always take your mobile computing equipment on as hand luggage when traveling by air and keep the equipment within view when going through security.
- 7) Protect your passwords Do not under any circumstances write down any of your user IDs or passwords on the equipment itself or on materials that are left in the storage bag.

Missing/lost/stolen mobile computing equipment must be reported immediately to **AHW Infrastructure Management at (780) 415 1600.** Missing/lost/stolen mobile computing equipment that contains restricted, confidential, or protected information must **also** be reported to the **Manager of Information Security and Compliance at (780) 427 8089**.

10. Key Contacts

Security

•	AHW Help Desk	(780) 917 4141
•	Manager, Information	(780) 427 8089
	Security and Compliance	
•	AHW Infrastructure	(780) 415 1600
	Management	



 Manager, Privacy (780) 422 8642

All Media

Senior Records Officer	(780) 415 2786
------------------------	----------------

Physical Security

•	Building Security	(780) 408 1920
•	AHW Physical Security	(780) 427 1465





11. Online Resources

Health Information Act http://www.qp.gov.ab.ca/documents/Acts/

H05.cfm

HIA Regulation http://www.qp.gov.ab.ca/documents/Regs

/2001_070.cfm

Freedom of Information and

Protection of Privacy Act

http://www.qp.gov.ab.ca/documents/Acts/

F25.cfm

Government Organization Act

G10.cfm

http://www.gp.gov.ab.ca/documents/Regs

/2001 224.cfm

Records Management

Regulation

http://www.im.gov.ab.ca/publications/pdf/

http://www.gp.gov.ab.ca/documents/Acts/

TransitoryRecordsSchedule.pdf

Transitory Records Retention and Disposition Schedule

http://www.im.gov.ab.ca/publications/pdf/

ARDA.pdf

Administrative Records Disposition Authority

http://www.im.gov.ab.ca/publications/pdf/
OfficialTransitoryRecordsGuide.pdf

Official and Transitory Records: A Guide for Government of Alberta

Employees

https://www.sharp.gov.ab.ca/secure/DocD

isplay.cfm?DocID=2356

Security Policy for Disk Wiping Surplus Computers

Code of Conduct & Ethics for the Public Service of Alberta

http://www.pao.gov.ab.ca/Practitioners/?fil

e=legreg/code/titlepage

AHW Security intranet site

http://intranet.health.gov.ab.ca/Reddot/34

0.htm

Use of Government of Alberta Internet and E-mail

http://www.pao.gov.ab.ca/?file=directives/

relations/use-of-information

AHW Password Standard

http://intranet.health.gov.ab.ca/Reddot/34

0.htm



12. Glossary

Affiliate Refer to the Alberta <u>Health Information Act</u> for the definition of an Affiliate.

AHW Alberta Health and Wellness

Availability The premise that information is consistently available for authorized users, entities,

or processes when needed to fulfil their business and legal obligations.

Confidentiality The premise that information is not made available or disclosed to unauthorized

individuals, entities, or processes.

Custodian Refer to the Alberta Health Information Act for the definition of a Custodian.

FOIP Freedom of Information and Protection of Privacy Act

Health Information "Means any or all of the following:

i) diagnostic, treatment, and care information;

ii) health services provider information;

iii) registration information;"

HIA Health Information Act

Individually identifying "When used to describe health information (as defined in HIA), means that the

identity of the individual who is the subject of the information can be readily

ascertained from the information."

Information Combinations of data used to support specific business needs found in both

databases and documents.

Information Security The protection of information resources from accidental or intentional unauthorized

collection, access, disclosure, modification, or destruction, or the inability to use that

information.

Record "Means a record of (health) information in any form and includes notes, images,

audiovisual recordings, x-rays, books, documents, maps, drawings, photographs,

letters, vouchers and papers and any another information that is written,

photographed, recorded or stored in any manner, but does not include software or

any mechanism that produces records."

Risk The likelihood or probability that a loss of information resources or breach of

security will occur.

Security Incident An actual or suspected case where information resources are compromised.

Staff Include all employees of AHW, student placement, and other casual short-term

appointments.

Third parties Persons who are not AHW staff. Third parties comprise:

Information Managers and other custodians under HIA

Hardware and software maintenance and vendor support staff and outsourcers.



Virus

Any malicious software that executes in a manner that damages, destroys, or prevents use of normal business operations. Malicious code programs, e.g., Trojans, are particularly dangerous to confidentiality as they allow remote control, or interception of information, without the user's knowledge.

For additional information, please contact:

Alberta Health and Wellness Information Policy and Compliance Unit

(780) 427 8089

Information Security Classification Scheme Table

	Level	Consequences of inappropriate	Safeguards/Countermea	Storage Criteria:	Transfer:	Disposal:	Examples:	Accountability for
		disclosure, alteration or	sures used to protect					use/ disclosure
		destruction:	this classification:					

	Level	Consequences of inappropriate disclosure, alteration or destruction:	Safeguards/Countermea sures used to protect this classification:	Storage Criteria:	Transfer:	Disposal:	Examples:	Accountability for use/ disclosure
High	1 Re- stricted	Loss of Confidentiality- If the information was disclosed AHW would be in breach of regulations or would be legally liable to a business partner, stakeholder, patient, or employee relations with business partners or vendors would be negatively impacted. Business partner seriously harmed, measured by loss of business or loss of competitive position. Business partner may no longer share information with AH&W. reputation with patients, stakeholders would be damaged. Loss of public confidence in AHW. AHW employee morale would be negatively impacted. AHW would lose competitive advantage or "trade secrets". the security of other Restricted of Confidential systems could be affected. Loss of Privacy: OIPC investigation Order from OIPC for remedial action Fines under HIA Loss of Availability: if the information was rendered unavailable critical, time-dependent business function(s) would be impaired. could cause a malfunction of other systems or processes	 Access to Restricted information assets is granted to specific individuals or roles with the required level of consent. Authority for modification to this class of information is also limited to specific users or roles possessing the required level of consent. Encryption must be used to protect the information when it is transmitted or stored outside the highly secure zone. All access or actions to information asset will be logged and subject to non-repudiation processes as appropriate. No unauthorized copies/print outs may be made 2-factor authentication outside of AHW "trusted" network No public physical access to areas where information is stored/ in use 	 Encrypt data Store in safe Store in Highly Secure Zone Provide access on need to know basis only Do not leave info. unattended Lock info. in desk when not in use 	 Encrypt data Courier transport supervise d by staff Never fax 	Shred, with certification Destroy data media, with certification	Budget information Minister-DM correspondence	Deputy Minister or ADM Person who created record (Only applicable for user created office documents i.e. Word, Excel)

L	Level Consequences of inappropriate disclosure, alteration or destruction:	Safeguards/Countermea sures used to protect this classification:	Storage Criteria:	Transfer:	Disposal:	Examples:	Accountability for use/ disclosure
	Loss of Integrity: If the information was altered • business related reports of personal health information could be misrepresented. • public statements would be in error (annual report). • poor business decision could be made • business processes could be disrupted or slowed • it alteration is undetected it may be difficult to correct or to revert to backup records	information in electronic mail transmission (email) is prohibited. Restricted information must not be placed on PC local storage without additional security provisions such as password protection and encryption.					

Level	Consequences of inappropriate disclosure, alteration or destruction:	Safeguards/Countermea sures used to protect this classification:	Storage Criteria:	Transfer:	Disposal:	Examples:	Accountability for use/ disclosure
2 Confidential	 Loss of public confidence in AH&W OIPC investigation Order from OIPC for remedial action Fines under HIA Disciplinary action 	 Confidential information assets are limited for access to the users who have a valid identification and have been authenticated and are operating in the role authorized to access Confidential information. Authority for modification to this class of information may be limited to specific users or roles possessing the required level of consent. Encryption must be used to protect the information when it is transmitted to a zone that is classified as an external zone. Encryption must always be used to protect information when it is transmitted to locations over a public or untrusted network. Confidential information contained or attached to email transmission must be protected with cryptographic techniques to protect the confidentiality and integrity of these electronic messages. 	Keep out of sight if away from desk Lock info. in desk at the end of the day Control access to work area with reception	Send by courier Confirm fax number and confirm receipt Encrypt data in public zone	Shred Destroy data media	Individually identifying health/personal information	Information / Application Steward Person who created record May 30

Confidential
 information must not

	Level	Consequences of inappropriate disclosure, alteration or destruction:	Safeguards/Countermea sures used to protect this classification:	Storage Criteria:	Transfer:	Disposal:	Examples:	Accountability for use/ disclosure
	3 Internal Use Only	EmbarrassmentMischief	 Need to know policies Password protected screen savers Single-factor authentication 	Lock information in desks when not in use Control access to work area with reception	 Regular mail Regular e-mail Confirm fax number Interoffice mail 	 Shred Delete and empty 'Recycle Bin' folder 	 Non-identifying personal/health information Drafts of documents that will become public 	 Information / Application Steward or Program Manager Current user of file
Low	4 Public	This information is considered to be in one of the above categories until released.	Care should be taken to protect the integrity of information published electronically to prevent unauthorized modification which could harm the reputation of AHW Available in public areas (brochure racks, website, library) Controls in place to prevent unauthorized modification	Store near reception areas for easy access	E-mail Regular mail Inter-office mail	Recycle Delete	Publicly available documents Press releases Historical information (i.e. 15 years old)	Any staff Program area

- 1. **Restricted** is used for information that would be damaging to the integrity, image, or effective operation of the AH&W if improperly used or disclosed. Restricted may also be used for information requiring specific consent for access. Access to Restricted information is specific to an individual and very limited.
- 2. **Confidential** is used for information that must be protected from unauthorized disclosure or modification. Confidential information may include personal information, financial information or details concerning the effective operation of AH&W. Access to Confidential information is specific to a function, group or role.
- 3. **Internal Use Only** is used for information that is of interest to AH&W and must be protected from unauthorized access. Internal Use Only information is available to those possessing an authenticated identity.
- 4. **Public** is used for information that has no security access requirements and can be publicly shared without restriction.

Information Classification standards

This section documents the four classification levels used to classify AHW information assets and the protective security controls each classification must have in place.

X = Required 0 = Optional n/a = not applicable

Security Requirement	Restricted	Confidential	Internal Use	Public
Strong Authentication (Hardware Token) to Network from external location	×	×	×	
Simple Authentication (Userid and Password) to the Operating System (e.g. Windows 2000, NT)	×	×	×	
Simple Authentication (Userid and Password) to the Application(s)	×	×	×	
Authorization (permissions) granted by group or role		×	×	
Authorization (permissions) granted only by the individual	×			
Access Logged		×	0	
Access Logged with non-reputable identity	×			
Encrypted when transmitted/stored within the Highly Secure zone	0	n/a	n/a	n/a
Encrypted when transmitted/stored in or to/from Internal zone	×	0	0	
Encrypted when transmitted/stored in or to/from External or Public zone	×	×	×	

Health and Wellness Provincially Reportable Incident Response Process

Provincial Reportable Incident Response Process

Prepared by:

Information Compliance and Access Unit Information Management Branch

Document History

Version	Version Date	Summary of Changes	Author
1.0	August 2005	Initial document	AHW Privacy and Security Office
1.01	13 February 2007	Updates for pharmacy incident	AHW IPC unit
1.02	October 2009	Refresh initial document	AHW ICA Unit

Document Reviewers

Name	Date	Initials
Security Manager, Information Security and Compliance, ICA Unit, HSPIM, AHW		
Senior Manager, ICA Unit, HSPIM, AHW		

Document Approvers

Name	Date	Initials
Executive Director, IM, HSPIM, AHW		
Assistant Deputy Minister and Chief Information Officer, HSPIM, AHW		
Information Management/IT Strategic Committee (IMC)		

AHW Protected version 1.02 September 2009 Page 1 of 10

Provincial Reportable Incident Response Process

Table of Contents

Document History	. 1
Document Reviewers	. 1
Document Approvers	. 1
Table of Contents:	. 2
Introduction	. 3
Purpose	
PRÎRP Phases:	
1. Incident Detection and Recording Phase	.4
2. Classification and Initial Support Phase	. 5
3. Investigation and Diagnosis Phase	. 5
4. Resolution and Recovery Phase	6
5. Post incident Review Phase	
6. Incident Closure Phase	
7. Appendix (Definitions of Breaches)	

Introduction

Owned and managed by the AHW, the Provincial Reportable Incident Response Process (PRIRP) has been designed to ensure that all health stakeholders are aware of all possible threats to health data and how to respond to a suspected or real threat.

The Provincial Reportable Incident Response Process involves health stakeholders and the Incidence Response Team comprises members of the following:

- Health stakeholder such as Community Custodians;
- Alberta Health Services:
- Alberta Health and Wellness, which includes the ICA Unit, AHW Information Management Senior Managers;
- *Other external stakeholders* such as the public, the Office of the Information and Privacy Commissioner, the Alberta Medical Association, and the College of Pharmacy.

Any of these organizational groups or providers may report a suspected incident to health data. In addition, Alberta Health and Wellness may include these stakeholders in the ongoing communications related to the incident as determined by the *Provincial Reportable Incident Response Team (IRT)*.

Purpose

The PRIRP has been designed to ensure that health stakeholders are aware of all possible threats to health data and how to respond to a suspected or real threat.

The PRIRP provide guidance to all organizations as to the definition of what AHW considers a valid threat to health data. This guidance is summarized below:

Breach of Data Confidentiality – A breach of data confidentiality occurs when either a user views patient records he/she is not authorized to, or when any amount of data stored on electronic media is misplaced.

Breach of Data Integrity – A breach of data integrity is when any amount of incorrect data appears in the Alberta Netcare systems has the potential to affect patient safety.

Breach of Data Availability – A breach of data availability is when access to EHR systems is unavailable.

PRIRP Phases:

The PRIRP is divided into six phases:

- 1. Detection and Recording
- 2. Classification and Initial Support
- 3. Investigation and Diagnosis
- 4. Resolution and Recovery
- 5. Post Incident Review

AHW Protected version 1.02 September 2009 Page 3 of 10

6. Incident Closure

A high level description of each phase is provided below:

- *Incident Detection and Recording* identify incident owner and recording source of any suspected threat to health data;
- Classification and Initial Support technical review to confirm validity of suspected threat and activation of initial support by Incident Response Teams. This is basically the Incident ownership, monitoring, tracking and communication preparation phase
- *Investigation and Diagnosis* monitoring, tracking, communication, and implement measures to mitigate the threat and determine cause of problem;
- Resolution and Recovery identify weaknesses to existing processes and make strategic recommendations:
- *Incident Closure* verification of the initial categorization that was assigned to the incident, stakeholder is notified, and then incident is closed.
- *Post Incident Review* implement recommendations from Review phase and ensure changes are effective.

The PRIRP has communication links between Alberta Health and Wellness and the affected health stakeholder in each phase of the process. In addition, there are internal communication links with AHW senior management, who will direct any external communications as required.

IRT will be responsible for directing the entire process as depicted by the following steps:

1. Incident Detection and Recording

This is when the stakeholders or Alberta Health and Wellness (AHW) become aware that there is a *potential* threat to health data.

1.1 "Suspect Threat" – At this point, any stakeholder has a reasonable suspicion that there is a potential threat to health data. The stakeholder should **not** wait until there is proof of an incident. The stakeholder should immediately notify AHW and institute a parallel response in their organization.

If you suspect a threat to the confidentiality, availability or integrity of health data, please contact the Information Compliance Unit Security Manager at AHW. Security @gov.ab.ca or EHR Helpdesk at 1.877.931.1638 or 780.412.6778.

At the "Suspect Threat" phase, part of the mandate of AHW is to monitor EHR usage. During the monitoring, if AHW notices a potential threat, AHW will contact the affected stakeholder and begin an investigation.

- 1.2 ICAU Records Incident Upon receiving notification of a potential threat to health data, the AHW ICA Unit will record the Incident and initiate the PRIRP process immediately to engage IRT. At this point, the IRT coordinator will initiate communication and update the Response Team accordingly. The Response Team will consist of members of the ICA Unit, AHS, and other Health stakeholders as appropriate.
- 1.3 "Alert" The IRT will alert the senior management at AHW through the internal reporting process of the potential threat to health data.

AHW Protected version 1.02 September 2009 Page 4 of 10

1.4 "Notify Potential Threat" – Notify external stakeholders such as Office of Information and Privacy Commissioner (OIPC) of potential threat to health Information.

2. Classification and Initial Support

Assemble IRT and initiate support, confirm details, and gather data from the source of incident or the incident owner.

- 2.1 "Initiate Support" The initial support occurs after the potential threat has been validated. In this phase, the Incident Response Team is activated and begins to work to mitigate the problem. IRT will ensure that all required personnel are working on the incident. The affected health stakeholder will also activate their own response team at this point.
- 2.2 "Alert" senior management will be updated periodically of the results of the investigation and mitigation work. Senior management will be responsible for authorizing communication alerts and updates as required.
- 2.3 "Notify Significant Stakeholders?" Based on the information gathered, AHW senior management may elect to provide an update to various unaffected external organizations at this time.

3. Investigation and Diagnosis

The investigation is likely to involve various technical and operational staff members who are able to perform the technical analysis necessary to determine the incident impact.

- 3.1.1, "Conduct Joint Investigation" All potential threats will be investigated by IRT and a parallel investigation will be performed by the incident owner (health stakeholder). There will be constant communication between IRT and the Incident owner. The goal of these investigations is to determine whether or not a breach has occurred, which might impact to confidential health information. The Privacy Risk Assessment (PRA) tool can be utilized to determine whether to notify affected individuals.
- 3.2.1 "Root Cause Analysis and Diagnosis" After the necessary steps have been taken to mitigate the threat, a detailed root cause analysis will be performed by all appropriate technical team members within the incident owner's affected systems. The goal of this analysis will be to determine the exact cause of the problem and to develop a detailed plan of how to ensure the problem does not reoccur. Senior management will be updated periodically of the results of the root cause analysis performed by both IRT and the health stakeholder. Senior management may authorize communication alerts and updates as required.
- 3.1.2 "Alert" Senior management will be notified of the results of the Investigation and Root Cause Analysis. Senior management will be responsible for authorizing communication alerts and updates as required.
- 3.1.3 "Notification of Significant Stakeholder" Based on the severity of the problem and the information gathered, IRT team will decide on severity of the incident and

AHW Protected version 1.02 September 2009 Page 5 of 10

responsibility for notification of external stakeholder AHW senior management may elect to notify the public and/or provide an update to various external organizations (e.g. OIPC) at this time.

4. Resolution and Recovery

This is where the actual remediation of the problem is completed and where the detailed analysis of the cause of the problem occurs. The end of the Resolution & Recovery Response phase is marked by the implementation of the necessary fixes.

- 4.1.1 "Implementation of tactical solution Implement Short Term Controls" The IRT will work closely with the incident owner regardless to monitor the incident and in determining the actual data or systems that may have been breached. The resolution reached will be communicated to the incident owner and controls to mitigate the risks implemented forthwith. But more importantly this step implements any fixes outlined from the Root Cause Analysis. At this point, senior management may decide to restore access to the application or system. The necessary fixes may occur in systems or processes controlled by the health stakeholder, AHW, or both organizations.
- 4.1.2 "Alert" Senior management will be updated periodically of the results of the mitigation steps taken by both AHW and the health stakeholder. Senior management will be responsible for authorizing communication alerts and updates as required.

5. Post Incident Review

The Review phase requires all affected parties to review the incident and determine what, if any, policies, process or procedures need to be implemented or changed as a result of the incident.

5.1 "Incident Review" – The review needs to reflect on all aspects of what caused the incident, how the Response Teams responded to the incident, the reporting of the incident and any subsequent communications that occurred as a result of the incident.

The outcome of the Incident Review is a list of measurable technical and process changes that can be implemented in the health stakeholder organization to help ensure similar incidents do not occur again in the future. In addition, the review may recommend changes to improve the response process itself. It is important to ensure that the changes are measurable to ensure that the change has been effective before incident closure phase.

5.2 "Update OIPC" – AHW senior management may either update the OIPC or provide a documented Incident Report at the next scheduled meeting, or as urgent as possible.

6. Incident Closure

The purpose of this phase is to ensure that the technical and process changes recommended from the Post Incident Review phase have been implemented. In addition, the Incident Closure phase will review the measures to ensure that positive changes have been made. As a result, the Strategic Response phase may be several months in duration.

AHW Protected version 1.02 September 2009 Page 6 of 10

- 6.1 "Assign Responsibility to Action lessons learned". The changes incorporating all lessons learned (can be either for technical or business processes) are assigned to the identified owner to implement based on the recommendations from the Post Incident Review phase. The changes may need to be implemented by the incident owner/health stakeholder, AHW, or both.
- 6.2.0 Report: Track lessons learned, responsibilities and progress
- 6.2.1 "Provide Report to Significant Stakeholders?" Based on the information gathered, the IRT/senior management may elect to provide an update to various unaffected external organizations at this time.

AHW Protected version 1.02 September 2009 Page 7 of 10

Appendix

I. Definitions of Breaches

It is important to communicate what AHW has defined as a potential threat to the confidentiality, integrity or availability of health data, and what AHW considers to be the triggers and thresholds for Provincially Reportable Incidents. A Provincially Reportable Incident must be reported to AHW. Confidentiality triggers and thresholds for a Provincially Reportable Incident occur whenever there is a potential for a patient safety issue or when there is a significant number of affected records. Another possible breach of data confidentiality is loss of data stored on electronic media. AHW **must** be notified by the health stakeholder that a breach of data confidentiality has occurred immediately.

A breach of data confidentiality:

Breach of data confidentiality includes a user viewing health records of individuals that are not in the care of the user without written consent, or viewing records of public figures, celebrities, or the public at large without need to know. There is no minimum number of unauthorized accesses that will constitute a breach of confidentiality; however the number of unauthorized accesses will determine the magnitude of the response. Accidentally accessing a single record by entering incorrect patient data is not considered to be a breach of data confidentiality.

A breach of data integrity:

Breach of data integrity can be caused by system or human error. Normal data entry errors that will be corrected by quality assurance processes do not constitute a breach of data integrity. Any errors that cause a patient safety issue will be considered a breach of data integrity; however the number of affected records may determine the magnitude of the response. Integrity triggers for a Provincially Reportable Incident occur whenever there is a potential patient safety issue or when there is a significant number of affected records.

A breach of data availability:

Availability triggers for a Provincially Reportable Incident are any outage that will cause a potential patient safety issue or an outage of more than 15 minutes to EHR systems that do not directly affect patient safety. This typically will initiate business continuity or disaster recovery plans in the affected organization. However, poor performance of EHR systems is not considered a Provincially Reportable Incident, but still may be investigated by AHW, the health stakeholder, or both organizations.

II. Privacy and Security Incident Reporting Template

Purpose

To allow individuals to report Privacy and Security incidents or suspected incidents so that AHW responsibilities related to the protection of privacy and security are fulfilled, and to assist AHW in determining the cause of the actual or suspected incidents so that necessary changes are made to prevent future occurrences.

AHW Protected version 1.02 September 2009 Page 8 of 10

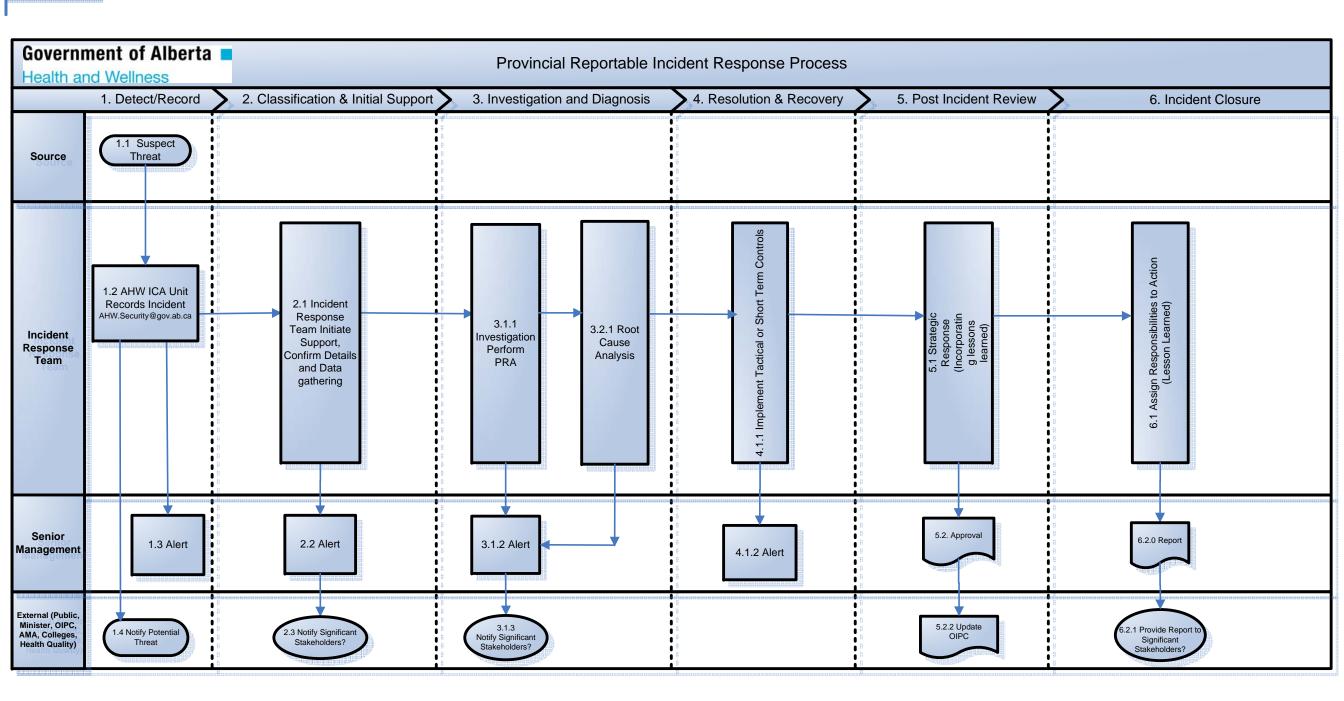


If you have any questions or prefer to report an incident by phone call *EHR Helpdesk at* 1.877.931.1638 or 780.412.6778 or contact the ICA Unit at 780-427-8089; or complete this form and email it to ahw.security@gov.ab.ca.

Subject to any overriding legal obligations, all information on this form is protected. You may be contacted by the Information Compliance and Access (ICA) Unit during Incidence Reponse.

Incident Information									
Incidence Reference number		Incident name			Incident Short Description:				
Incident Initially detected By:					Date/Time ncident occurred		Program/ Business Area Affected		
Asset Affected		Affected Number of Individuals		of		Risk rating assigned to this incident b Program/Business area (High, Mediu			
Incident Contact	Perso	n (for com	munica	tion	and f	ollow-u	ps)		
Name	Job Ti	tle	Phone		Fax			E-mail	
Incident Details									
Immediate Incident Mitigation									
Additional Comments/Notes									

AHW Protected version 1.02 September 2009 Page 9 of 10



Alberta Health and Wellness	POLICY					
FOIP Office	Approved by:					
Topic: Administration of the Freedom of	Paddy Meade Deputy Minister					
Information and Protection of Privacy						
(FOIP) Act						
Date Approved: June 12, 2007						

Part 1

Authority

The principal authorities governing administration of the *FOIP Act* are derived from:

- Freedom of Information and Protection of Privacy Act
- Health Information Act
- Records Management Regulation
- Public Service Act
- Code of Conduct and Ethics for the Public Service of Alberta

Policy Intent

It is the intent of the Department to comply with all aspects of the FOIP Act relating to receiving and responding to requests for personal, general, correction of personal requests and protecting the privacy of individuals.

This policy provides direction to the FOIP Office, delegated decision-makers and all other department staff regarding established roles and responsibilities.

Definitions

Annotation

A note that is added to a record by way of comment or

explanation.

Affiliates of AHW Agencies, Boards, or Commissions (ABC's)

The Act applies to both the Department as well as "public bodies" affiliates (agencies, boards,

committees, task forces, review panels) that report to the Minister of AHW. If agencies, boards, etc. have been dissolved or privatized, their records fall under the custody or control of the department (Appendix

"A").

Control (of record)

Authority to manage the record, including restricting, regulating and administering its use, disclosure or

disposition.

Custody (of record)

Having physical possession (i.e., holding and

retaining) of the record.

Disclose (personal information)

To release, transmit, reveal, expose, show, provide copies of, tell the contents of, or intentionally or unintentionally give personal information to someone by any means.

Disclose includes oral transmission of information by telephone or in person; provision of personal information on paper, by facsimile copy, or in any other format; and/or electronic transmission through electronic mail, data transfer, or the Internet.

Employee

In relation to a public body, includes a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body. For the purposes of the *Freedom and Information Act* and this policy, the term "employee" includes both an employee who has entered into a contract of employment or a person that has entered into a feefor-service contract.

Personal Information

Any recorded personal information about an identifiable individual.

Personal Information Bank

A collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual.

Manuals, Handbooks, or Guidelines

Any manual, handbook or other guideline used in decision-making processes that affect the public by employees of the public body in administering or carrying out programs or activities of the public body.

Part 2 General

Objectives and Principles of *FOIP*Act

All Alberta Health and Wellness (AHW) employees must understand and comply with the provisions of the FOIP Act, which has the following basic objectives and principles:

Objectives:

(Section 89(1) of the FOIP Act)

- To ensure that public bodies are open and accountable to the public by providing a right of access to records; and
- To protect the privacy of individuals by controlling the manner in which public bodies collect, retain, use, keep accurate, protect, disclose and dispose of personal information.

Principles:

- A right of access to records to establish a right of access by any person to records in the custody or under the control of the Department, subject to limited and specific exceptions, which are set out in the Act.
- Protection of personal privacy to protect personal information in our custody and control and ensure disclosure is accurate.
- A right of access to an individual's own personal information to create
 a right of access for individuals to personal information about
 themselves, again subject to limited and specific exceptions set out in
 the Act. Public bodies should interpret the exceptions with a view to
 giving an individual as much access as possible to his or her own
 personal information.
- A right to request a correction to allow individuals a right to request corrections to personal information about themselves that is held by a public body.
- Independent review of decisions to provide for the independent review
 of decisions made by public bodies under the Act and for the
 investigation of complaints. Independent review is provided by the
 Information and Privacy Commissioner.

The Act applies to all records in the custody or control of the Department, regardless of the medium in which the information is recorded or stored.

Part 3

Administration

3.1 FOIP Coordinator/ FOIP Office

The FOIP Coordinator is responsible for the overall management of access to information (personal, general and correction) and protection of privacy under the FOIP Act which includes:

- Comply with the access to information provisions contained in Part 1 of the FOIP Act and with the standards that follow. The Act requires the Department to, among other things, conduct a full search for responsive records, respond to requests within legislated timelines, assist the applicant as necessary, create records from electronic data if possible and fully consider any requested waiver of fees chargeable under the Act. Carrying out these requirements would include;
 - 1. Implement policies, guidelines, and procedures to manage the compliance with the provisions of the *FOIP Act*.
 - 2. Provide advice on the implementation and administration of the *FOIP Act* to the Department staff.
 - 3. Managing the process of FOIP requests by tracking, transferring, extending, and responding for general, personal, or correction or amendment of an individual's own personal information.
 - 4. Comply with the protection of privacy provisions contained in Part 2

- of the *FOIP Act*, regarding the disclosure and management of personal information.
- 5. Ensuring consistency in the application of other acts and regulations which relate to the prohibition or restrictions on disclosure of information.
- 6. Maintain list of all boards, committees and councils established by AHW and whether they should be included in the list of agencies, boards, commissions, corporations, offices or other bodies designated as public bodies.
- 7. Maintain list of any manual, handbook or other guideline used in decision-making processes that affect the public by employees of the public body in administering or carrying out programs or activities of the public body. (Section 89(1) of the FOIP Act)
- 8. Educate and train all AHW employees on the FOIP Act

3.2 Requests for Correction of Personal Information

Under section 36(1) of the FOIP Act, an individual who believes that his or her personal information, in the custody and control of AHW, contains an error or omission may request AHW to correct the individual's personal information.

Requests for Correction are subject to the same rules as requests for access under the Act. This includes time limits and Appeals by the Commissioner.

3.3 Formal Requests to Disclose Information

Under the *FOIP Act* anyone can ask for records (subject to limited and specific exemptions under the Act) in the custody or under the control of the Department.

A formal FOIP request is required when there is no legislation or policies and procedures that allow for release, or the records/information contains personal information, privileged information or third party personal information that require formal notice prior to disclosure. The FOIP request process is managed by the FOIP office.

Employees must not dispose of any records relating to a FOIP request after it is received, even if the records are scheduled for destruction under an approved records retention and disposition schedule.

3.4 Duty to Assist the Applicant/ Create New Records for disclosure

Under section 10(1) of the FOIP Act, AHW and the FOIP office must make every reasonable effort to assist the applicants and to respond to each applicant openly, accurately and completely. AHW obligations continue throughout the FOIP process.

Furthermore, under section 10(2) of the FOIP Act, the delegated head must create a record for an applicant if it is not an unreasonable interfere with the operations of the Department or could be generated by normal hardware, software, and technical expertise.

The FOIP Office should be consulted when a request has been made or there are plans to create new records for release. This consultation will determine whether these new records could be subject to a routine disclosure or breech of the Act.

3.5 Routine Disclosure of Personal Information

Routine disclosure, in response to a routine inquiry or request, occurs when access to a record can be granted without a request under the FOIP Act. Disclosure often takes place in limited and specific circumstances under program legislation (e.g., *Health Information Act*) or under Section 40 of the *FOIP Act*.

Program areas must where possible consult with the FOIP Office to determine which types of records would qualify for routine disclosure.

All routine disclosures must have legislative authority along with:

- 1. Established guidelines, manuals or policies.
- 2. Verification of the identity of the individual to whom the information is disclosed or ensure that individual's authorized representatives provide appropriate evidence of their right to exercise that individual's right.
- 3. Documentation of disclosure. (Documentation should include what information is being disclosed, to whom, when it was disclosed and the subsection(s) of the legislation that authorized the disclosure)

A formal FOIP request would be required to obtain personal information for non-routine disclosures or when the FOIP or other applicable legislation would not allow disclosure of the requested information in this manner.

3.6 Protection of Personal Information

Personal information of individuals in the custody or under the control of the Department is protected by the privacy provisions of the *FOIP Act*. The information can only be collected, used or disclosed in accordance with the FOIP Act and must be kept reasonably secure. Reasonable efforts must be taken to ensure the accuracy and completeness of personal information that is used to make a decision that impacts an individual. Please see attached delegation table for specific responsibilities (Appendix "B")

3.7 Disclosure in Public Interest

Whether or not a request is made, the Deputy Minister of Alberta Health and Wellness is delegated the obligation to disclose the following information, including personal information if necessary; and without delay:

- information about a risk of significant harm to the environment or to the health or safety of the public, an affected group of people, a person or the applicant; or
- information of the disclosure which is, for any other reason, clearly in the public interest.
- The health information relates to the possible commission of an offence under a statute or regulation of Alberta or Canada.

Part 4	Delegation and Responsibilities			
4.1 Delegation of Authority	The Delegation of Ministerial Powers under the <i>FOIP Act</i> (Appendix "B") lists duties, powers or functions delegated to individuals filling specific positions. Only these Delegated Authorities can carry out the specified responsibilities.			
4.2 Minister responsibility	The "head" (Minister) of the public body may delegate to any person, duty, power, or function of the head under the Act, <u>except</u> the power to delegate under section 85(1) of the FOIP Act.			
4.3 Deputy Minister Responsibility	 Authority to confirm or deny the existence of records under section 12(2) of the Act. Approve the release of records that relate to Cabinet and Treasury Board Confidences under section 22(1) of the Act. Approve the release of records that relate to a matter of "Public Interest" under section 32(1) of the Act. 			
4.4 ADM/ Directors	ADM/Exec. Directors are responsible for ensuring that the Department's responsibilities under the <i>FOIP Act</i> are clearly communicated to, and are understood and adopted by their employees. However, the Waiver of any fees charged under the Act as per section 87(4) of the Act has been delegated to the HR/FOIP Executive Director for the FOIP office (Delegation matrix- Appendix "B")			
4.5 Offences and Penalties	The FOIP Act contain provisions that allow for the application of penalties to individuals for offences for willful breaches of management of personal information and other activities of non-compliance.			
	 Any loss of personal information or breach of personal privacy is considered to be a sensitive breach. Any breach must be reported immediately to the designated senior official and to the Privacy Manager of the Information Strategic Services Division (ISSD). 			
Part 5	Investigation and Audits			
5.1 Appeal, Investigations, and Reviews	The Office of the Information and Privacy Commissioner (OIPC) will launch a Review, Appeal, or Mediation on complaints from individuals about any matter pertaining to the FOIP Act request for Information.			
	The FOIP Coordinator acts as the official contact for all communications to or from the Commissioner's Office on these matters. The FOIP Coordinator, Legal Counsel, and/or program area are required to work collaboratively to address the questions or issues raised by the OIPC.			
Part 6	General Provision (Part 6 of the FOIP Act)			
6.1 Directory of public bodies	The FOIP Coordinator must publish, in printed or electronic form, a directory to assist in identifying and locating records. The directory must list each public body which includes:			

the name and business contact information of the individual that is
the public body's contact person for matters relating to the
administration of the FOIP Act or if the public body does not have a
contact person for matters relating to the administration of the FOIP
Act, the name and business contact information of the head of the
public body.

6.2 Personal Information Bank

The FOIP Coordinator must maintain and publish a listing of personal information banks in the custody or under the control of the Department. This listing provides a public record of the purposes for which the personal information may be used or disclosed and includes the following information:

- the title and location of the personal information bank;
- a description of the kind of personal information and the categories of individuals whose personal information is included;
- the authority for collecting the personal information in the personal information bank; and
- the purposes for which the personal information is collected or compiled and the purposes for which it is used or disclosed.

All ADMs and Directors must ensure that all plans to create new records with personal information are reported to the FOIP office so that this directory is kept current

6.3 Access to Department Manuals

Under section 89(1) of the FOIP Act, the public body must provide facilities at the headquarter of the public body and any offices of the public body that, in the opinion of the head, are reasonably practicable, where the public may inspect any manual, handbook, or other guidelines used in decision-making processes that affect the public by employees of the public body in administering or carrying out programs or activities of the public body.

Any information in a record that the delegated head of a public body would be authorized to refuse to give access to pursuant to the FOIP Act may be excluded from the manuals, handbooks, or guidelines that may be inspected pursuant to subsection (1)

Part 7 Training and Awareness

The FOIP Office will develop and make available training and awareness materials and workshops to orient and train all new staff as to their responsibilities relative to the Act.

It is the responsibility of all Ministry/Department staff to be informed about the rules contained in the Act and to understand how they impact the collection, management, use and disclosure of information.

Program managers and supervisors must ensure and assess their staff duties and determine the appropriate level of training and awareness regarding FOIP.

Part 8 General Guidelines

Guidelines

Anonymity of the applicant – Under the Act, the identity of the applicant should be disclosed only:

- to those officials and employees of AHW who have a need to know it in order to carry out their job duties; and
- to the extent necessary to carry out the FOIP functions in processing the applicant's request.
- The identity of applicants requesting their own personal information will be shared within the department on a need to know basis only.

Consultation – To achieve consistency across government and to develop an informed recommendation to the Head for approval, a highly consultative approach will be used in responding to FOIP requests. The FOIP Office will consult with other levels of government, other departments or agencies, third parties potentially impacted by the release of the records, program area authors of the records, program managers, legal advisors within Alberta Justice, Communications Branch, and others as necessary.

Destruction of records – When the department receives a FOIP request, disposition or destruction of records potentially responsive to the request will not occur until the request has been responded to and the potential appeal timelines have passed. Anyone who destroys records to evade a FOIP request (i.e. prior to or after receipt of the request) can be found guilty of an offense under the Act and personally fined an amount up to \$10,000.

Receipt of FOIP requests – Alberta Health and Wellness is officially in receipt of a FOIP request when either the FOIP Office, or the Minister's Office, receives it. All employee's must alert the FOIP Office immediately upon receipt of a FOIP request form, correspondence indicating that information is being requested under the FOIP Act, or correspondence referencing matters regarding the administration of the Act.

Release into the public domain – Information released in response to a FOIP request enters the public domain. As the Department will not have any control over subsequent use or disclosure of the information, including publication or broadcast by the media, caution in decision-making regarding release must be exercised.

Required response times – Alberta Health and Wellness will respond to FOIP requests within legislated time limits. To achieve this objective, all potentially responsive records will be located by the business units and provided to the FOIP Office as quickly as possible, but no later than 3-5 working days from the date of notification to begin searching for the

records. Subsequent review and approval of proposed FOIP response packages is to be on an "as soon as possible" basis.

Third party business information – As Alberta Health and Wellness must continue to receive a wide variety of corporate information related to the Health professionals, propriety information (i.e. Pharmaceutical companies) and other regulatory matters to fulfill its mandate, all third party business interests will be protected to the extent possible under the Act. Utilizing the FOIP process will ensure a more thorough examination of any potential harm associated with the disclosure have been addressed and involving the third party, the FOIP office, Legal & Legislative Services and the Office of the Information and Privacy Commissioner (if necessary).

Personal information – As Alberta Health and Wellness must continue to receive a wide variety of personal information related to the Health and Wellness's mandate, all personal information must be protected to the extent possible under the Act. Utilizing the FOIP process will ensure a more thorough examination of any potential harm associated with the disclosure of personal information have been addressed and the appropriate program areas are involved prior to disclosure.

Training and awareness – The FOIP Office will develop and make available training and awareness materials and workshops to orient and train staff as to their responsibilities relative to the Act. The Ministry and/or Department staff are responsible to be informed about the rules contained in the Act and to understand how they impact the collection, management, use and disclosure of information. Program managers and supervisors will ensure that their staff have the appropriate level of training and awareness regarding FOIP.

Delegation – Specific decision making powers, responsibilities and ability to act are delegated according to the FOIP delegation of authority instrument approved by the Minister. (Appendix "B")

FOIP Request Response Procedure

- 1. Once a request is received by the FOIP Office or the DM/Minister's Office, the department has 30 calendar days (22/23 working days) in which to respond to the request.
- 2. The FOIP Coordinator sends out a broadcast e-mail message to the ADM's of each division (cc: EA's) to advise that a request has been received. This e-mail serves as a notification ONLY. Recipients are to reply to the FOIP Office once a request for records is received (electronic or hardcopy- Blue Folder) if they have or might have any potentially responsive records to the request. Recipients are also to ensure that any records destruction activity that may have been in progress ceases.
- 3. The FOIP Office will clarify the wording of the request with the

- applicant and will attempt to narrow the scope of the request to minimize the operational impact on the Department and reduce the cost of a response to the applicant.
- 4. Once the request has been clarified, the FOIP Office will advise the program area and require the program area to conduct a detailed search of records responsive to the request. Program areas are to search for records and provide a copy of all <u>potentially responsive</u> records to the FOIP Office within 3-5 working days. Response times longer than this standard must be negotiated directly with the FOIP Office. Program areas are to consult with the FOIP Office if there is any question as to whether a record is responsive to a request or if the projected search time is excessive (i.e. over 6 hours). Fees may need to be collected from the applicant prior to conducting the search.
- 5. The FOIP Office, in consultation with the program area, will review all records to determine which records are sensitive and/or responsive to the request and where exceptions to disclosure within the FOIP Act may apply.
- 6. The FOIP Office will consult with other parties, obtain legal advice as necessary and obtain or apply any necessary time extensions to the requested response.
- 7. The FOIP Office will prepare and provide recommendations to the program area regarding possible release of records under the Act. Program area concurrence with the recommended approach is required before the file is forwarded for approval to release.
- 8. The FOIP Office obtains approval to release the FOIP package from the delegated authority.
- 9. The FOIP Office informs the Communications Branch of the content and timing of release so the appropriate officials may be briefed in advance.
- 10. The FOIP Office provides a formal response to the applicant.

APPROVED		
Original signed by		
Paddy Meade	June 12, 2007	
Deputy Minister	Date	

Provisions of the FOIP Act and Regulation for which Delegation of Authority Should be Considered (Part 1)

Administrative Responsibilities in the FOIP Act and Regulation that May be Assigned (Part 2)

Duty, power or function of public body	Section reference	Retained by Head	Assigned to FOIP Coordinator	Assigned to other person (Provide title(s) – specific or generic)
Right of Access				
Establishing process for receiving access requests	2(a), (c)		V	
Assuring process for access is made public	Regulation 2(1)		V	
Authority to declare request abandoned	8(1)		V	
Authority to grant continuing request	9(2)		√	
Duty to assist applicants	10(1)		$\sqrt{}$	
Duty to create records	10(2)			HR/FOIP Executive Director, ADM, COMM Director
Authority to decide on content of response/ grant or refuse access	11 & 12(1)			HR/FOIP Executive Director, ADM, COMM Director
Authority to refuse to confirm or deny the existence of a record	12(2)			DM

Duty, power or function of public body	Section reference	Retained by Head	Assigned to FOIP Coordinator	Assigned to other person (Provide title(s) – specific or generic)
Authority to decide how access will be given	13 Regulation 3		V	
Authority to extend time limit	14(1) & 14(3)		$\sqrt{}$	
Authority to request Commissioner's permission for extension	14(1) & 14(2)		V	
Authority to transfer a request for access	15		√	
Exceptions				
Authority to withhold information harmful to business interests of a third party	16			HR/FOIP Executive Director, ADM, COMM Director
Authority to withhold information harmful to personal privacy	17			HR/FOIP Executive Director, ADM, COMM Director
Authority to withhold information harmful to individual or public health or safety	18 Regulation 5(1),(3),(5)			HR/FOIP Executive Director, ADM, COMM Director
Authority to withhold confidential evaluations	19			HR/FOIP Executive Director, ADM, COMM Director
Authority to withhold information harmful to law enforcement	20			HR/FOIP Executive Director, ADM, COMM Director

Duty, power or function of public body	Section reference	Retained by Head	Assigned to FOIP Coordinator	Assigned to other person (Provide title(s) – specific or generic)
Authority to withhold information harmful to intergovernmental relations	21			HR/FOIP Executive Director, ADM, COMM Director
Authority to withhold Cabinet confidences	22			DM
Authority to withhold local public body confidences	23			HR/FOIP Executive Director, ADM, COMM Director
Authority to withhold advice from officials	24			HR/FOIP Executive Director, ADM, COMM Director
Authority to withhold information harmful to economic interests of a public body	25			HR/FOIP Executive Director, ADM, COMM Director
Authority to withhold testing procedures, tests and audits	26			HR/FOIP Executive Director, ADM, COMM Director
Authority to withhold privileged information	27(1) & (2)			HR/FOIP Executive Director, ADM, COMM Director
Authority to withhold information harmful to conservation of heritage sites or endangered species	28			HR/FOIP Executive Director, ADM, COMM Director
Authority to withhold information that is or will be available to public	29			HR/FOIP Executive Director, ADM, COMM Director

Duty, power or function of public body	Section reference	Retained by Head	Assigned to FOIP Coordinator	Assigned to other person (Provide title(s) – specific or generic)
Third Party Interve	ention			
Duty to give third party notice	30		√	
Authority to decide whether to give access to third party information	31(1)			HR/FOIP Executive Director, ADM, COMM Director
Duty to give notice of decision	31(2)–(4)		V	
Public Interest				
Authority to disclose information in public interest	32(1)			DM
Duty to give notice to third party, Commissioner	32(3), (4)		V	
Collection, Accurac	ey and Retention	n of Personal Inf	ormation	
Establishing controls over the collection, use and disclosure of personal information	2(b)			HR/FOIP Executive Director, ADM, COMM Director
Authorizing routine correction of personal information	2(d)		V	
Ensuring authorized purpose of collection	33			HR/FOIP Executive Director, ADM, COMM Director
Assuring proper collection and notification	34			HR/FOIP Executive Director, ADM, COMM Director

Duty, power or function of public body	Section reference	Retained by Head	Assigned to FOIP Coordinator	Assigned to other person (Provide title(s) – specific or generic)
Assuring accuracy of personal information	35(a)			HR/FOIP Executive Director, ADM, COMM Director
Applying retention standards	35(b)			HR/FOIP Executive Director, ADM, COMM Director
Collection, Correct	ion, Protection	of Personal Info	rmation	
Authority to set aside collection requirements	34(3)			HR/FOIP Executive Director, ADM, COMM Director
Authority to decide on requests for correction of personal information	36(1)		√	
Duty to correct, annotate or link personal information, duty to notify previous recipients	36(3), (4)		V	
Duty to give notice to individual requesting correction	36(7)		V	
Authority to transfer a request for correction	37		V	
Duty to ensure protection of personal information	38			Information Manager
Use and Disclosure of Personal Information				
Establishing rules for electronic consent	Regulation 6(5)(a)			HR/FOIP Executive Director, ADM, COMM Director

Duty, power or function of public body	Section reference	Retained by Head	Assigned to FOIP Coordinator	Assigned to other person (Provide title(s) – specific or generic)
Establishing rules for oral consent	Regulation 6(6)(a)			HR/FOIP Executive Director, ADM, COMM Director
Assuring appropriate uses	39			HR/FOIP Executive Director, ADM, COMM Director
Assuring proper disclosures of personal information	40 (May be different for each provision)			ADM (in accordance with Part 2)
Disclosing in accordance with Part 1	40(1)(a)		V	
Disclosing if not an unreasonable invasion of third party's personal privacy	40(1)(b)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing for original or consistent purpose	40(1)(c)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing after individual consents	40(1)(d)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to comply with enactment of Alberta or Canada or treaty, arrangement or agreement made under enactment	40(1)(e)			HR/FOIP Executive Director, ADM, COMM Director
Signing personal information sharing agreements	40(1)(e)			HR/FOIP Executive Director, ADM, COMM Director

Duty, power or function of public body	Section reference	Retained by Head	Assigned to FOIP Coordinator	Assigned to other person (Provide title(s) – specific or generic)
Disclosing in accordance with enactment of Alberta or Canada that authorizes or requires disclosure	40(1)(f)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to comply with subpoena, warrant or court order	40(1)(g)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing where necessary for employee of public body or member of Executive Council to perform duties	40(1)(h)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing where necessary for delivery of common or integrated program or service	40(1)(i)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to enforce legal right of Government of Alberta or public body	40(1)(j)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to collect debt or fine or make payment	40(1)(k)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to determine or verify eligibility for program or benefit	40(1)(1)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to Auditor General and other prescribed persons for audit purposes	40(1)(m)			HR/FOIP Executive Director, ADM, COMM Director r

Duty, power or function of public body	Section reference	Retained by Head	Assigned to FOIP Coordinator	Assigned to other person (Provide title(s) – specific or generic)
Disclosing to Member of Legislative Assembly to assist individual	40(1)(n)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to bargaining agent acting on behalf of employee	40(1)(o)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing for archival purposes	40(1)(p)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to assist investigation	40(1)(q)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing from one law enforcement agency to another law enforcement agency	40(1)(r)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to next of kin or friend of injured, ill or deceased individual	40(1)(s)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to expert under section 18(2) to protect individual or public safety	40(1)(u)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing for legal proceedings to which Government of Alberta or public body is a party	40(1)(v)			HR/FOIP Executive Director, ADM, COMM Director

Duty, power or function of public body	Section reference	Retained by Head	Assigned to FOIP Coordinator	Assigned to other person (Provide title(s) – specific or generic)
Disclosing through Minister of Justice and Attorney General to place of lawful detention	40(1)(w)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to manage or administer personnel	40(1)(x)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to enforce a maintenance order	40(1)(y)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to officer of the Legislature where necessary to carry out duties	40(1)(z)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing for supervision of individual under control of correctional authority	40(1)(aa)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing when information available to the public	40(1)(bb)			Information Manager
Disclosing business contact information	40(1)(bb.1)			Information Manager
Authority to disclose to relative or adult interdependent partner of deceased individual	40(1)(cc)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to lawyer acting for an inmate	40(1)(dd)			HR/FOIP Executive Director, ADM, COMM Director

Duty, power or function of public body	Section reference	Retained by Head	Assigned to FOIP Coordinator	Assigned to other person (Provide title(s) – specific or generic)
Authority to disclose to avert imminent danger to health or safety	40(1)(ee)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing to administrator of Motor Vehicle Accident Claims Act	40(1)(ff)			HR/FOIP Executive Director, ADM, COMM Director
Post-secondary educational body only: disclosing alumni information for its own fundraising activities and ADM or HR/FOIP Executive Director or COMM Director Administering disclosure agreements	40(2)			HR/FOIP Executive Director, ADM, COMM Director
Post-secondary educational body only: disclosing teaching and course evaluations	40(3)			HR/FOIP Executive Director, ADM, COMM Director
Disclosing for research and statistical purposes and for ADM or HR/FOIP Executive Director or COMM Director Administration of research agreements	42 & 43			HR/FOIP Executive Director, ADM, COMM Director

Duty, power or function of public body	Section reference	Retained by Head	Assigned to FOIP Coordinator	Assigned to other person (Provide title(s) – specific or generic)
Authority to approve conditions for disclosure for research and statistical purposes and for ADM or HR/FOIP Executive Director or COMM Director Administration of research agreements	42(c)			HR/FOIP Executive Director, ADM, COMM Director
Authority to disclose to guardian of a minor	84(1)(e)			HR/FOIP Executive Director, ADM, COMM Director
Reviews and Comp	laints			
Authority to ask the Commissioner for advice	54(1)		V	
Authority to request Commissioner to disregard requests	55		V	
Authority to require Commissioner to examine original record on site	56(4)		V	
Right to make representations to the Commissioner	69(3), (5), (6)		V	
Duty to discharge burden of proof	71		V	
Duty to comply with Commissioner's Order	74	_	√	

Duty, power or function of public body General Provisions	Section reference	Retained by Head	Assigned to FOIP Coordinator	Assigned to other person (Provide title(s) – specific or generic)
Duty to publish a directory of the body's personal information banks and keep it current	87.1(1) and (4)		V	
Duty to record uses or disclosures of personal information not included in directory	87.1(3)		√	
Authority to specify categories of records available without formal request and require a fee	88		√	
Duty to make manuals available	89		V	
Fees				
Authority to assess and collect fees	93		V	
Authority to waive fees	93(4)			HR/FOIP Executive Director
Duty to give notice of decision to grant or refuse waiver request	93(4.1)		V	

Alberta Health and Wellness	POLICY
FOIP/HIA Office	Approved by:
Topic: Administration of the Health	Paddy Meade Deputy Minister
Information Act (HIA)	
Date Approved: June 12, 2007	

Policy Intent

It is the intent of the department to comply with all aspects of the HIA relating to receiving and responding to requests for health information, correction of health information and protecting the health information of individuals under <u>Part 2</u>, <u>Part 6</u> and <u>Part 7</u> of HIA.

This policy provides direction to the FOIP/HIA Office, senior decision-makers, affiliates and all other department staff (i.e. Contract employees) regarding established roles and responsibilities under HIA.

Definitions

FOIP/HIA Office All requests for access to health information or the

correction of health information are managed by the

FOIP/HIA Office and its staff.

Custodian A "custodian" is an organization or individual in the

health system who receives and uses health

information and is responsible for ensuring that it is protected, used, and disclosed appropriately (defined

in section 1(1)(f) of HIA).

Affiliates An individual employed by the custodian.

Control (of record)

Authority to manage the record, including restricting, regulating and administering its use, disclosure or

disposition.

Custody (of record)

Having physical possession (i.e., holding and

retaining) of the record.

Disclose (health information)

To release, transmit, reveal, expose, show, provide copies of, tell the contents of, or intentionally or unintentionally give health information to someone by

any means.

Disclose includes oral transmission of information by telephone or in person; provision of personal information on paper, by facsimile copy, or in any other format; and/or electronic transmission through electronic mail, data transfer, or the Internet.

Health Information

Any and all of the following: 1). diagnosis, treatment, and care information; 2). Health services provider information; 3). Registration information.

Section 1

General

The FOIP/HIA Coordinator is responsible for the overall management of access to health information (Parts 2, 6, and 7) and the policy direction relating to the protection of health information under HIA is the responsibility of Information Policy and Compliance (IPC) unit.

Section 2

Administration

2.1 FOIP/HIA Coordinator and FOIP/HIA Office

- Comply with the access to health information provisions contained in Parts 2, 6, and 7 of the HIA. The Act requires the department to, among other things, conduct a full search for responsive records, respond to requests within legislated timelines, assist the applicant as necessary, create records from electronic data if possible and fully consider any requested waiver of fees chargeable under the Act. Carrying out these requirements would include;
 - 1. Managing the process for tracking and responding to requests for access and correction or amendment of an individual's own health information.
 - 2. Ensuring consistency in the application of other acts and regulations which relate to the prohibition or restrictions on disclosure of health information.
 - 3. Comply with the access to health information provisions contained in HIA.
 - 4. All disclosures of health information made by the individual or to the individual's authorized representative must be verified by the FOIP/HIA office to ensure the identity of the individual to whom the information is being disclosed, and to ensure that individual's authorized representatives provide appropriate documentation of their right to exercise that individual's right under the Act.
 - 5. Determining applicable fees to be charged for services provided under Part 2 of *HIA*, must be in accordance with sections 9, 10, 11 and the schedule of the *Health Information Regulation*.
 - 6. The FOIP/HIA office will handle the privacy issues and follow-up to an access or correction request under HIA. The Information Policy and Compliance (IPC) unit is generally responsible for the protection of privacy under HIA such as: collection, use, security, and Privacy Impact Assessments (PIA's).

2.2 Requests for Correction of Health Information

The FOIP/HIA Coordinator is responsible for the overall management process of correcting health information. Individuals have the right to request corrections to health information about themselves that is held by a custodian.

The custodian must respond to the request for correction within 30 days of

receiving it in the HIA office or provide a notice of extension under section 13(2) of HIA. There may be situations where the correction may not be possible, including those where there is no concrete basis for the correction, or if a request is made to correct an opinion. In such situations the HIA office must respond with an annotation to the file.

Also, any corrections to health information on a record must be passed on to other individuals who may have been given a copy of the record or information within the past year.

2.3 Create New Records for Disclosure

The FOIP/HIA Office should be consulted when there are plans to create and disclose new types of health information maintained by the department or custodian (AHW). This consultation will determine whether these new records could be subject to routine disclosure or active dissemination without a formal HIA request.

2.4 Routine Disclosure of Health Information

All disclosures of health information must be authorized by legislation. Disclosure often takes place in limited and specific circumstances under program legislation. However, disclosing health information must be in compliance of HIA

If a custodian discloses individually identifying diagnostic, treatment, and care information without the consent of the individual who is the subject of the information as per section 35(1) or (4) of HIA, a disclosure notion must be maintained for a period of ten years following the date of disclosure. This notation must include a description of the information that is being disclosed, the name of the person, to whom the information is being disclosed, and the date and purpose of the disclosure.

If there is no legislation, guidelines or policies in place that allows the disclosure of health information to be released, the Program areas must where possible consult with the FOIP/HIA Office to determine which types of records would qualify for routine disclosure.

Unauthorized or non-compliance disclosures of health information may result in an appeal, complaint or investigation by either the individual the information is about or the Office of the Information and Privacy Commissioner.

Section 3 Responsibilities 3.1 Assignment of Responsibility under the HIA- Parts 2, 6, and Part 7 Responsibility Table The Assignment of Responsibility under the HIA- Parts 2, 6, and Part 7 (Appendix A) lists duties, powers and functions assigned to individuals fulfilling specific positions. The affiliates are responsible for ensuring that the custodian's responsibilities under the HIA are clearly communicated to, and are understood and adopted by each user.

3.3 Offences and Penalties

Deputy Minister

The *HIA* contain provisions that allow for the application of penalties to individuals for offences of willful breaches of management of health information and other activities of non-compliance.

Date

Any loss of health information or breach of HIA is considered to be a sensitive breach. The breach must be reported immediately to the Information Policy and Compliance unit using the AHW Privacy and Security Breach Investigation Form.

Section 4	Investigation and Appeals
4.1 Investigations and appeals	The Office of the Information and Privacy Commissioner (OIPC) will launch an appeal on complaints from individuals about their access request or correction to their health information.
	The FOIP/HIA Coordinator acts as the official contact for all communications to or from the Commissioner's Office on these matters.
APPROVED Original signed by	
Paddy Meade	June 12, 2007

Health Information Act (HIA) ASSIGNMENT OF RESPONSIBILITY TABLE

Duty, power or function of Custodian	Section Reference	Assigned to the Affiliates	Assigned to FOIP/HIA Coordinator	Assigned to other person (Title)
Part 2 Individual's Right to Access	Individual's H	Health Informa	ation	
Right of individual to access individua	l's health infori	nation		
Any record containing health information about individual in custody or under control of custodian.	7(1)		√	
Does not extend to information a custodian is authorized or required to refuse access under section 11, unless information can be severed from a record.	7(2)		√	
Subject to the payment of any fee required by the regulations.	7(3)		√	
How to make a request				
Individual must make the request to the custodian who has custody or control of the record.	8(1)		V	
Under subsection (1) the custodian may require the applicant to submit the request in writing.	8(2)		V	
In a request applicant may ask for a copy or examine the record.	8(3)		V	
Abandoned request				
When custodian contacts applicant in writing seeking further information necessary to process request or requesting applicant to pay a fee or agree to pay a fee.	9(1)		V	
Notice declaring a request abandoned must state that applicant may ask for review of decision by Commissioner.	9(2)		V	
Duty to assist applicants		T		
Custodian has received request for access to record under section 8(1)	10		√	
Right to refuse access to health inform	ation	,		
Custodian may refuse to disclose health information to an applicant.	11(1)		√	
Custodian must refuse to disclose health information to an applicant	11(2)		\checkmark	
Time limit for responding to a request	for access			
Custodian must respond to a request within 30 days of receiving it under section 8(1) or within any extended period under section 15	12(1)		V	
In a response under subsection (1), the custodian must tell the applicant;	12(2)		V	

Duty, power or function of Custodian	Section Reference	Assigned Information Affiliates	Assigned to FOIP/HIA Coordinator	Assigned to other person (Title)
---	----------------------	---------------------------------------	----------------------------------	---

Correction or amendment of health info	rmation	,
Individual who believes an error or omission in their health information may in writing request the custodian that has it in its custody or under its control to correct or amend the information.	13(1)	√
Within 30 days of receiving request under subsection (1) or within extended period under section 15 the custodian must decide whether it will make or refuse correction or amendment.	13(2)	√
If custodian agrees to make correction or amendment, it must be done within the 30-day period or any extended period under subsection (2).	13(3)	√
Custodian not required to provide notification referred to in subsection (3) where the custodian agrees to make the correction or amendment but believes that the applicant will not be harmed if notification under subsection (3)(c)is not provided and the applicant agrees.	13(4)	√
If custodian refuses to make correction/amendment, they must give written notice to applicant within 30-day period or any extended period referred in subsection (2) and reasons for refusal.	13(5)	√
Custodian may refuse to make correction/amendment that has been requested in respect of:	13(6)	√
Failure to respond to a request in accordance with this section within the 30-day period or any extended period referred to in subsection (2) to be treated as refusal.	13(7)	√
Refusal to correct or amend information		
Where custodian refuses to make correction/amendment under section 13, they must tell applicant that they may elect to either of the following, but may not do both	14(1)	√
Applicant who submits statement of disagreement must do so within 30 days of receiving written notice of refusal. Under section 13(5) or within any extended period under section 15(3)	14(2)	√
On receiving the statement of disagreement, the custodian must if reasonable, attach the statement of record that is the subject of the requested correction or amendment, and provide a copy of the statement of disagreement to any person to whom the custodian has disclosed the record in the year preceding the applicant's request for the correction or amendment.	14(3)	

Duty, power or function of Section Reference	Assigned Information Affiliates	Assigned to FOIP/HIA Coordinator	Assigned to other person (Title)
--	---------------------------------------	----------------------------------	---

Extending time		
Custodian may extend time for responding to request under section 8(1) or 13(1) for additional period up to 30 days or, with Commissioner's permission for longer period if;	15(1)	√
If time extended under subsection (1), custodian must tell applicant;	15(2)	√
Commissioner may extend time within which applicant must submit statement of disagreement under section 14(2) if in opinion of Commissioner;	15(3)	V
Request under s8 or s13 deemed to be a	request under	FOIP
If written request made under section 8(1) for access to record containing information which FOIP Act applies, part of request relating to that information deemed to be request under section 7(1) of FOIP Act and it applies to that part of request as if it had been make under section 7(1)	16(1)	V
Written request made under section 13(1) to correct/amend information to which FOIP Act applies it is deemed to be request under section 36(1) of FOIP Act, that Act applies to request as if it had been made under section 36(1)	16(2)	V
This section does not apply if custodian that receives request is not a public body as defined in the FOIP Act	16(3)	V
Existing procedures still available		
Individual not limited to procedure set out in this part to request access to health information about individual if another procedure available	17	V

<u>Part 6</u>			
Power to charge fees			
Custodian may charge fees provided for in regulations for services provided under Part 2	67(1)	√	
Subsection (1) does not permit custodian to charge fee in respect of request for access to applicant's own health information, except for cost of producing copy	67(2)	V	
Custodian must give applicant estimate of total fee for services before providing them.	67(3)	$\sqrt{}$	
Custodian may excuse applicant from paying all or part of fee, if, in opinion of custodian, applicant cannot afford fee or any other circumstances in regulations	67(4)		HR/FOIP Executive Director

Duty, power or function of Custodian	Section Reference	Assigned Information Affiliates	Assigned to FOIP/HIA Coordinator	Assigned to other person (Title)
If applicant requested custodian to excuse them from paying all or part of fee and custodian has refused their request, custodian must notify applicant they may ask for review by Commissioner	67(5)		V	
Fees referred to in subsection (1) must not exceed actual cost of services	67(6)		V	
Part 7 Commissioner				
Right to ask for a review	73(1)		V	
How to ask for a review	74(1)		√	
Notifying others of review	75(1)		V	
Mediation may be authorized				
Commissioner may authorize mediator to investigate and attempt to settle any matter subject of request for review	76		V	

Alberta Netcare Data Availability Table (as of December 4, 2009)

DRUG DATA (PIN) Prescriptions 2 Allergies and Intolerances 2 Dispensed Drugs 2 LAB DATA AHS - Cancer 1 Provincial Lab 2	20-Mar-06 20-Mar-06 20-Mar-06 20-Mar-06 10-May-06 04-May-07 20-Mar-06 20-Mar-06	1-Mar-93 26-Jun-05 1-Mar-02 1-Dec-99 1-Jul-04 24-Mar-06 24-Apr-07 1-Dec-04	Identifier Numbers and Demographic data for people registered through Alberta Health with a provincial Personal Health Number (PHN) and/or Unique Lifetime Identifier (ULI) Includes Prescriptions entered by physicians into the PIN application as we as "Inferred" Prescriptions generated from Pharmacy Batch Dispenses. Allergies and intolerances entered by physicians into the PIN application All dispenses for Group 66 (seniors program) patients until December 2007 After that time, all medications submitted as part of participating pharmacies' batch Dispense records submitted from participating pharmacies through pharmacy batch. Excludes hospital pharmacy on discharge. As of October 2009, an average of 92% of all prescription dispenses expected on a monthly basis are being added to the Portal. Cross Cancer Institute lab data Tom Baker Centre lab data from CLS
DRUG DATA (PIN) Prescriptions 2 Allergies and Intolerances 2 Dispensed Drugs 2 LAB DATA AHS - Cancer 1 Provincial Lab 2	20-Mar-06 20-Mar-06 20-Mar-06 20-Mar-06 10-May-06 04-May-07 20-Mar-06	26-Jun-05 1-Mar-02 1-Dec-99 1-Jul-04 24-Mar-06 24-Apr-07 1-Dec-04	Alberta Health with a provincial Personal Health Number (PHN) and/or Unique Lifetime Identifier (ULI) Includes Prescriptions entered by physicians into the PIN application as we as "Inferred" Prescriptions generated from Pharmacy Batch Dispenses. Allergies and intolerances entered by physicians into the PIN application All dispenses for Group 66 (seniors program) patients until December 2007 After that time, all medications submitted as part of participating pharmacies' batch Dispense records submitted from participating pharmacies through pharmacy batch. Excludes hospital pharmacy on discharge. As of October 2009, an average of 92% of all prescription dispenses expected on a monthly basis are being added to the Portal. Cross Cancer Institute lab data Tom Baker Centre lab data from CLS
Prescriptions 2 Allergies and Intolerances 2 Dispensed Drugs 2 LAB DATA AHS - Cancer 1 Provincial Lab 2	20-Mar-06 20-Mar-06 20-Mar-06 10-May-06 04-May-07 20-Mar-06	1-Mar-02 1-Dec-99 1-Jul-04 24-Mar-06 24-Apr-07 1-Dec-04	as "Inferred" Prescriptions generated from Pharmacy Batch Dispenses. Allergies and intolerances entered by physicians into the PIN application All dispenses for Group 66 (seniors program) patients until December 2007 After that time, all medications submitted as part of participating pharmacies' batch Dispense records submitted from participating pharmacies through pharmacy batch. Excludes hospital pharmacy on discharge. As of October 2009, an average of 92% of all prescription dispenses expected on a monthly basis are being added to the Portal. Cross Cancer Institute lab data Tom Baker Centre lab data from CLS
Allergies and Intolerances 2 Dispensed Drugs LAB DATA AHS - Cancer Provincial Lab 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	20-Mar-06 20-Mar-06 20-Mar-06 10-May-06 04-May-07 20-Mar-06	1-Mar-02 1-Dec-99 1-Jul-04 24-Mar-06 24-Apr-07 1-Dec-04	as "Inferred" Prescriptions generated from Pharmacy Batch Dispenses. Allergies and intolerances entered by physicians into the PIN application All dispenses for Group 66 (seniors program) patients until December 2007 After that time, all medications submitted as part of participating pharmacies' batch Dispense records submitted from participating pharmacies through pharmacy batch. Excludes hospital pharmacy on discharge. As of October 2009, an average of 92% of all prescription dispenses expected on a monthly basis are being added to the Portal. Cross Cancer Institute lab data Tom Baker Centre lab data from CLS
2	20-Mar-06 20-Mar-06 10-May-06 04-May-07 20-Mar-06	1-Dec-99 1-Jul-04 24-Mar-06 24-Apr-07 1-Dec-04	All dispenses for Group 66 (seniors program) patients until December 2007 After that time, all medications submitted as part of participating pharmacies' batch Dispense records submitted from participating pharmacies through pharmacy batch. Excludes hospital pharmacy on discharge. As of October 2009, an average of 92% of all prescription dispenses expected on a monthly basis are being added to the Portal. Cross Cancer Institute lab data Tom Baker Centre lab data from CLS
Dispensed Drugs 2 LAB DATA AHS - Cancer Provincial Lab 2	20-Mar-06 10-May-06 04-May-07 20-Mar-06	1-Jul-04 24-Mar-06 24-Apr-07 1-Dec-04	After that time, all medications submitted as part of participating pharmacies' batch Dispense records submitted from participating pharmacies through pharmacy batch. Excludes hospital pharmacy on discharge. As of October 2009, an average of 92% of all prescription dispenses expected on a monthly basis are being added to the Portal. Cross Cancer Institute lab data Tom Baker Centre lab data from CLS
2	10-May-06 04-May-07 20-Mar-06	24-Mar-06 24-Apr-07 1-Dec-04	Dispense records submitted from participating pharmacies through pharmacy batch. Excludes hospital pharmacy on discharge. As of October 2009, an average of 92% of all prescription dispenses expected on a monthly basis are being added to the Portal. Cross Cancer Institute lab data Tom Baker Centre lab data from CLS
AHS - Cancer Co Provincial Lab 2	04-May-07 20-Mar-06	24-Apr-07 1-Dec-04	Tom Baker Centre lab data from CLS
AHS - Cancer Provincial Lab 2	04-May-07 20-Mar-06	24-Apr-07 1-Dec-04	Tom Baker Centre lab data from CLS
Provincial Lab 2	20-Mar-06	1-Dec-04	
			Posulte for ontire province including proposal LIV
	20-Mar-06	4 4 - 00	Results for entire province including prenatal HIV
	l	1-Apr-02	All AHS - Edmonton lab data (UAH labs and DKML/DynaLIFE)
AHS - Edmonton	20-Mar-06	1-Oct-04	DKML/DynaLIFE Microbiology data. Tests before Oct 1/04 will only display name of test, not results.
	20-Mar-06	17-Jun-05	Tuberculin Skin Tests (TST). All records that have a PHN/ULI in the Microbiology folder.
		24-Apr-07	General lab, microbiology, pathology and blood bank results from Calgary Laboratory Services. Excludes HIV & 4 special coagulation tests where display in Portal is clinically unacceptable.
		22-Jan-07	General lab, microbiology, pathology, blood bank results from Banff & Canmore
AHS - Calgary	04-May-07	20-Nov-07	General lab, microbiology, pathology, blood bank results from Didsbury
		4-Dec-07	General lab, microbiology, pathology, blood bank results from Strathmore
		8-Dec-08	General lab, microbiology, pathology, blood bank results from Okotoks, Hig River, Black Diamond, Vulcan, Claresholm
AHS - South	25-May-07	16-May-07	General Lab and Microbiology results from regional facilities. Medicine Hat Diagnostic Lab results added Dec-08 and are uploaded daily appearing th following morning after 8:30 a.m.
<u> </u>	28-Sep-07	13-Sep-07	Pathology results from regional facilities
	20-Jun-08 25-May-07	9-Jun-08 16-May-07	Blood bank results from regional facilities General Lab and Microbiology from regional facilities
	28-Sep-07	13-Sep-07	Pathology results from regional facilities
ALIC Control	30-Jun-08	9-Jun-08	Blood bank results from regional facilities
	20-Mar-06	1-Apr-02	DKML/DynaLIFEDX - General Lab & blood bank from Red Deer, Lloydminster & Smith Clinic Camrose. Microbiology back to Oct 1/04
2	25-May-07	16-May-07	General Lab from regional facilities
	29-Jun-07	29-Jun-07	Microbiology from regional facilities
	28-Sep-07	13-Sep-07	Pathology results from regional facilities
	20-Jun-08 20-Mar-08	9-Jun-08 1-Apr-02	Blood bank results from regional facilities All results from DKML/DynaLIFE. Microbiology back to Oct 1/04
Canadian Blood Services			Not submitting at this time
DIAGNOSTIC IMAGING DATA			
	20-Mar-06	1-Aug-03	DI text reports from all regional facilities
	20-Mar-06	14-Oct-03	DI text reports from UAH
	19-Nov-07	19-Nov-07	DI text reports from Stollery Children's Hospital
	20-Mar-06	12-Mar-04	DI text reports from RAH
	19-Nov-07 01-Dec-04	19-Nov-07 01-Dec-04	DI text reports from Glenrose Hospital DI text reports from Insight Medical Imaging
	01-Dec-04 01-Nov-04	01-Dec-04 01-Nov-04	DI text reports from Medical Imaging Consultants
	01-Jun-07	01-Jun-07	DI text reports from CML Healthcare



Alberta Netcare Data Availability Table (as of December 4, 2009)

Data Source	Date Available	Results Back To	Comments	
	01-Sep-07	01-Sep-07	DI text reports from Northgate Xray	
	01-Sep-07	01-Sep-07	DI text reports from Edmonton Cardiology Consultants	
	18-Sep-09	2-Jan-08	DI text reports from Amiha Diagnostics	
	28-Sep-07	14-Sep-07	DI text reports from all regional facilities.	
ALIC Colmoni	01-Oct-08	10-Oct-07	DI text reports from Elliot Fong Wallace Radiology	
AHS - Calgary	29-May-08	29-May-08	DI text reports from Radiology Consultants Associated	
	01-Oct-09	1-Oct-09	DI text reports from Canadian Medical Laboratories	
	25-Sep-09	25-Sep-09	DI text reports from Canadian Diagnostic Centres	
AHS - South	25-May-07	16-May-07	DI text reports from all regional facilities. No private community provider results at this time	
AHS - Central	25-May-07	16-May-07	DI text reports from all regional facilities and Smith Clinic in Camrose. No other private community provider results at this time.	
AHS - North	25-May-07	16-May-07	DI text reports from all regional and private facilities except Saddle Lake Health Centre and Associate Medical Clinic X-ray.	
			DI text reports from the Alberta Cancer Board (Cross Cancer Institute).	
AHS - Cancer	29-Jun-07	7-Jun-07	Tom Baker Centre does not have DI facilities so patients have DI performe by outside service providers.	
APPROACH (Alberta Provincial Project for Outcome Assessment in Coronary Heart Disease)	04-Dec-08	21-Nov-08	Includes Coronary Angiography and Percutaneous Coronary Intervention reports for the entire province.	
TRANSCRIBED REPORTS				
AHS - Edmonton	20-Mar-06	1-Jul-03	Includes Consultations (except from UAH), Discharge Summaries, Admission History, and Operative Reports from regional facilities except those identified below. Unable to quantify the consults etc that are not transcribed into Dictaphone.	
	16-Jun-08	16-Jun-08	Alberta Hospital Edmonton Admission Histories, Discharge Summaries an Consultations for Adult-General and Geriatric patients	
	27-Oct-08	27-Oct-08	Leduc Admission Histories, Discharge Summaries, Consultations and Operative reports	
	04-Nov-08	04-Nov-08	Westview and Devon Admission Histories, Discharge Summaries, Consultations and Operative reports	
	18-Nov-08	18-Nov-08	Redwater and Fort Saskatchewan Admission Histories, Discharge Summaries, Consultations and Operative reports	
	20-Mar-06	17-Mar-05	Community Care Client Profiles - displayed under Summary Reports folder	
AHS - South AHS - Central AHS - North	04-Dec-08	21-Nov-08	Includes Admission Histories, Discharge Summaries, Consultations, and Operative Reports	
AHS - Cancer	20-Oct-06	29-May-06	Physician Progress Notes, Admission Histories, Discharge Summaries, Initial Consultations (Cross Cancer Institute and Tom Baker Centre)	
	29-Jun-07	14-Jun-07	Operative Reports from Cancer Surgery Alberta for entire province (Cross Cancer Institute and Tom Baker Centre)	
AHS - Calgary	18-Sep-09	3-Sep-09	Consultations, Discharge Summaries, Admission Histories, Operative Reports and Procedure Reports from Calgary facilities	
PATIENT EVENT HISTORY				
AHS - Edmonton	20-Mar-06	1-Jan-96	Inpatient, outpatient and emergency events from all regional facilities.	
OTHER				
	20-Mar-06	1-Jan-96	Immunizations done at Public Health sites. Does not include Emergency of Private office. All records that have a PHN/ULI.	
	12-Jun-07	12-Jun-07	Emergency Dept discharge summaries from: Westview Health Centre, Devon General Hospital, Fort Saskatchewan HC (12-Jun-07)	
	31-May-07	31-May-07	Emergency Dept discharge summaries from Grey Nuns	
	07-Jun-07	07-Jun-07	Emergency Dept discharge summaries from Leduc	
	05-Jun-07	05-Jun-07	Emergency Dept discharge summaries from Misericordia	
	29-May-07	29-May-07	Emergency Dept discharge summaries from Northeast Community HC	
	14-Jun-07	14-Jun-07	Emergency Dept discharge summaries from Redwater HC	
AHS - Edmonton	22-May-07	22-May-07	Emergency Dept discharge summaries - Royal Alexandra Hospital	
	24-May-07	24-May-07	Emergency Dept discharge summaries - University of Alberta Hospital	
	13-Feb-07	13-Feb-07	ECG results from Sturgeon	
	04-Feb-08	04-Feb-08	ECG results from Misericordia	
	25-Oct-07	25-Oct-07	ECG results from University of Alberta	
			1	



Alberta Netcare Data Availability Table (as of December 4, 2009)

Data Source	Date Available	Results Back To	Comments	
	29-Apr-08	29-Apr-08	ECG results from Grey Nuns	
	02-Sep-08	02-Sep-08 ECG results from Leduc		
	15-Sep-09	15-Sep-09	ECG results from Royal Alexandra - Cardiology only Stress & Holter test results from Mazankowski Alberta Heart Institute	
	03-Dec-09	20-Nov-09		
AHS- Cancer	04-Dec-08	21-Nov-08	ECG results from Cross Cancer Institute.	

Overview of the ANP Data Sources and Repositories:

Netcare repositories housed in Edmonton

- o TREP Transcribed Reports Repository (Edmonton)
- o RREP Rural Report Repository
- CHRP Capital Repository which houses Edmonton zone immunizations, home care summaries and ADT events today

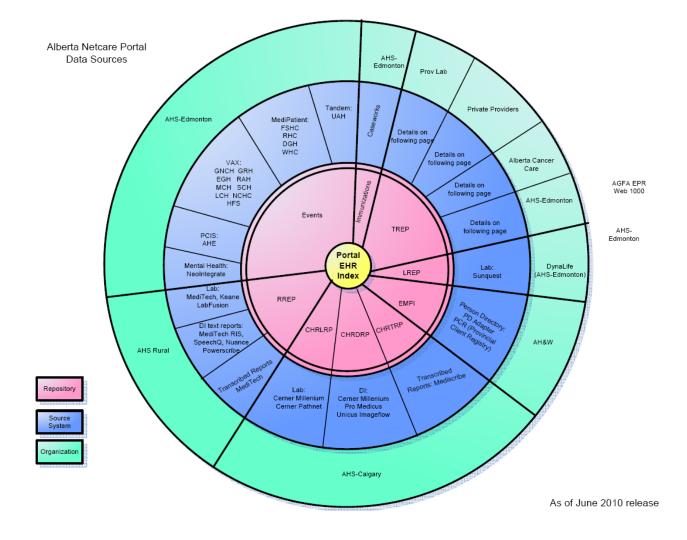
Netcare repositories housed in Calgary

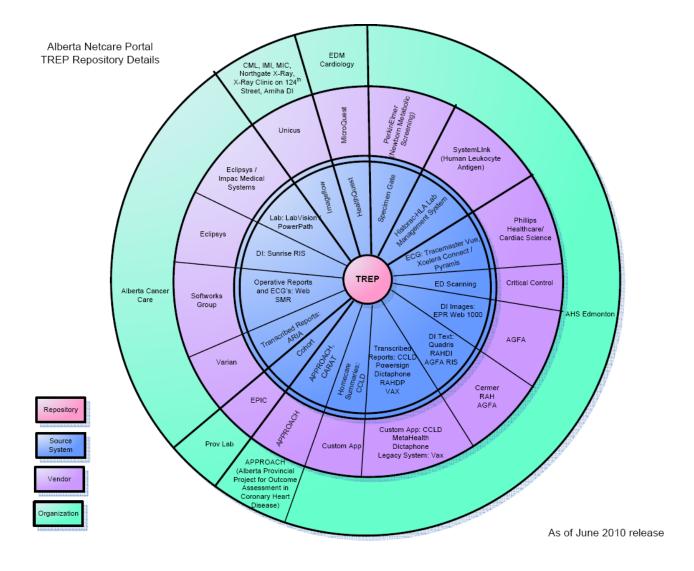
- CHRLRP Calgary Lab Repository
- CHRDRP Calgary Diagnostic Imaging Text Report Repository
- CHRTRP Calgary Transcribed Report Repository

Other repositories accessed by Netcare

- LREP Lab Repository (Edmonton) This repository is 'owned' by the Edmonton zone lab team and is used by Dynalife their lab provider. Netcare accesses it to view the lab results. This repository is not managed by ANP.
- CHPACS Capital Health (now Edmonton zone) Picture Archiving Repository this is not an ANP repository and is
 managed by the DI team. It is accessed via a launch of the application Web1000 in Edmonton only. The 'PACS'
 integration initiative will change this localized launch to allow access to both the Edmonton and Calgary DI/PACS
 repositories (all images provincially).

ACRONYM	FULL NAME
AHE	Alberta Hospital Edmonton
APPROACH	Alberta Provincial Project for Outcome Assessment in Coronary Heart Disease
CARAT	Coronary Artery Reporting and Archiving Tool
CCLD	Community Care Local Database
DGH	Devon General Hospital
DI	Diagnostic Imaging
ECG	Electrocardiogram
ED	Emergency Department
EGH	Edmonton General Continuing Care Centre
EMPI	Enterprise Master Patient Index
EPR	Enterprise Patient Record (AGFA acronym)
FSHC	Fort Saskatchewan Health Centre
GNCH	Grey Nuns Community Hospital
GRH	Glenrose Rehabilitation Hospital
HFS	Health First Strathcona
HLA	Human Leukocyte Antigen (Histocompatibility Lab)
IMI	Insight Medical Imaging
LCH	Leduc Community Hospital
MCH	Misericordia Community Hospital
MIC	Medical Imaging Consultants
NCHC	Northeast Community Health Centre
PCIS	Patient Care Information System
RAH	Royal Alexandra Hospital
RAHDI	Royal Alexandra Hospital Diagnostic Imaging
RAHDP	Royal Alexandra Hospital Dictaphone
RHC	Redwater Health Centre
RIS	Radiology Information System
SCH	Sturgeon Community Hospital
SMR	Surgical Medical Record
UAH	University of Alberta Hospital
WHC	Westview Health Centre







Provincial Organizational Readiness Assessment

Facility Name			
Site Name			
Site Contact			
Date of Assessment			
Regional Health Authority			
Vendor Name			
 the Custodian represents and warranamed facility and he/she has authen the information and representations the Custodian will immediately not contained herein; the Custodian acknowledges that and the Custodian agrees to complete the Custodian hereby gives consent deemed necessary by Alberta Health The Custodian further acknowledges are Alberta Health and Wellness may, we ensure continued compliance with the Upon completion of the assessment 	ants that he/she is signing cority to do so; is contained herein are comply Alberta Health and Welling and the second assessments may be those additional assessment to Alberta Health and Welling and Welling and Welling and Welling and Welling and Welling and the second assessment to a second assessment of the second agrees that: """ """ """ """ """ """ """	ness to collect, use and disclose the info the Custodian's access to Alberta Netcare. er, inspect and perform and audit on the Control ORA; and Custodian may be granted access to Alberta st be fulfilled to the satisfaction of Alberta F	nent; ion or representations te access to Regional systems ormation contained herein as ustodian's clinical systems to
Remarks			
Custodian or Delegated Representati	ve (Print Name)	Signature	Date
Security Officer (Print Name & Organ	ization)	Signature	Date

AWH Confidential (when completed)





Frequently Asked Questions

What is p-ORA?

- The p-ORA (Provincial Organizational Readiness Assessment) is a security assessment for sites that want to access Alberta Netcare applications. These community sites are not managed by a health region or board. Currently, Alberta Netcare is being deployed to physicians and pharmacies.
- It is a set of minimum administrative, physical and technical security requirements that when met will mitigate some of the risks associated with sites connecting to Alberta Netcare.
- It is divided into three sections; web access, system-to-system, and wireless sections.

Must all sites go through and pass all the three sections of the p-ORA?

- No, but all sites must go through and pass Section One.
- Sites that implement wireless technology must go through and pass Section Three.
- Regions that allow sites to remotely access their clinical systems may require sites to go through and pass the remote access section before remotely accessing regional systems. This is section is under development.

What is required for a site to be engaged with p-ORA process?

• A site must have a PIA (Privacy Impact Assessment) that has been accepted by the Office of the Information Privacy Commissioner or the PIA development must be in progress.

Who conducts the assessment?

 Alberta Health and Wellness, through the Alberta Netcare Deployment Team, conducts the p-ORA for access to provincial systems. Assessment for access to regional systems is the responsibility of the Regional Health Authorities.

If a site passes the p-ORA can the custodian access a regional system?

• Yes, but other requirements may apply as deemed necessary by the regions. Only one assessment will be conducted for sites that want to access both provincial and regional systems.

Who reviews and approves the p-ORA?

Alberta Health and Wellness reviews and approves the p-ORA for access to provincial systems.

What is the validity period for approved p-ORA?

Two years from the date of approval.

Will sites be audited after completing the p-ORA?

Alberta Health and Wellness reserves the right to audit sites at any time as deemed necessary.

How can I get more information about the p-ORA?

If you have questions or need more information about the p-ORA, please, contact the HIA Help Desk at **(780) 427 8089** or send an email to **AHW.security@gov.ab.ca**





Instructions

- All community sites must complete and meet the security requirements on section one of the Provincial ORA.
- All System to System (S2S) sites must complete and meet the requirements on both sections 1 and 2.
- In addition, all sites that implement wireless technology must complete and meet the requirements on section 3.

Note: This assessment is **NOT** required for sites where the workstations and networks are managed by the Health Region or Board or for sites that are Pharmacy Batch only.

Section One: Mandatory Security Requirements for all Accesses

Has a PIA been accepted by the Office of the Information Privacy Commissioner (OIPC)? If yes, state the date of acceptance.	Yes No [] [Double click box to check or uncheck]
	Acceptance Date:
Has an Information Manager Agreement been signed between the Custodian	Yes No
and AHW?	
Does your business have a wireless network? If yes, the wireless security	Yes No
assessment in this p-ORA must be completed. If an AHW wireless security	
assessment was completed and approved at least two years ago, a new	
assessment needs to be completed and approved. Please, state the date of	Date of approval of AHW wireless
approval of AHW wireless assessment.	assessment:





	Security Awareness and Training		
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?
1.1	If affiliates are not provided with appropriate and adequate security and Health Information Act (HIA) training, they will not know how to securely use health data. Consequently, health information could be accidentally disclosed to unauthorized individuals causing a breach of patient privacy. As the HIA mandates that the custodian protects health information, the custodian will be held responsible for being noncompliant with the HIA in the event of a breach.	 Provide initial training on office policies, security awareness and HIA compliance to new employees. Provide ongoing security awareness training using various means such as posters, flyers, etc. Provide ongoing training and updates on how the practice complies with HIA. Ensure each affiliate signs an oath of confidentiality or non disclosure agreement. Refresh this agreement bi-annually or during contract review. 	





	Security Administration			
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?	
1.2	The absence of a Security or Privacy Officer leads to security controls being improperly and inconsistently coordinated within the organization. There is lack of accountability in the event of a security incident. Also no one will be responsible for assessing the situation, taking corrective action and notifying the right parties in the event of a breach.	 Appoint a Security or Privacy Officer. Appoint an Access Administrator (AA). Clearly define the functions of the AA and the Security or Privacy Officer. Provide appropriate and ongoing training to the AA and/or Security or Privacy Officer. 		

	Security Policy		
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?
1.3	The absence of a well developed, well maintained and enforced security policy negatively affects the way security is implemented within an organization. The implementation of security controls will be inconsistent and tilted towards a more reactive approach than the preferred proactive approach. As a result, the risk that	 Develop a Security Policy for the organization. Use clear and simple language in the Security Policy document for easy understanding and interpretation by affiliates. Keep the security policy up-to-date. Enforce the security policy through regular audits and reviews. 	





health information could be viewed by unauthorized individuals or made unavailable when needed increases.	Cover security policy during security awareness and training.	
---	---	--

	Termination Process		
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?
1.4	Lack of a proper termination process could allow a terminated employee to have access to information processing systems or data. If a weakness in the termination process allows this scenario, health information could be improperly disclosed. This could cause patients' privacy to be breached.	 Develop and document an employee termination process. Make a comprehensive list of action items to be performed during an employee termination. Delete network or operating system and EHR user accounts. Revoke all access control items (keys, badges, access cards, fob, etc) must be revoked. Provide adequate and appropriate training to the individual responsible for implementing the termination process. Update the termination process document as appropriate. 	

Screen Locks and Monitor Orientation		
What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?
Computer terminals located or computer monitors facing publicly accessible areas pose	 Orient computer monitors such that unauthorized access to health information that may be displayed 	





1.5	a risk to patients' privacy as health information could be viewed by individuals who do not have a need-to-know. Also if computers in these areas are left unattended for a long period of time without appropriate security controls in place, the risk of health data being disclosed to unauthorized individuals increases.	on them is prevented. Physically separate reception areas from public access. Configure computer systems to timeout (screen lock) after a predefined period of user inactivity. Match timeout duration with the level of risk and exposure to such risk. To regain access to the system, a user should be prompted for his or her password.	
-----	--	---	--

	Software Installation		
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?
1.6	Uncontrolled installation of software within an organization's network environment exposes the network to malicious software codes such as viruses, Trojans, key loggers, spyware, etc. Some malicious codes are capable of taking screenshots, transferring data from a target computer to an attacker's computer, capturing and disclosing user logon credentials, corrupting data or disrupting services, etc. The risk of health data being viewed by unauthorized	 Develop and document a software installation process. Develop and enforce a security policy on software installation and ensure that it is covered during security awareness and training. Only install custodian or assigned delegate approved software. Keep and maintain an inventory of installed software as appropriate. Conduct a periodic review of installed software. Remove unneeded software completely from the environment. Protect the configuration settings of systems from being changed by 	





individuals increases.	non privileged users.
	 Provide non-privilege users with limited privilege accounts to prevent illegitimate installation of software.
	 Provide system administrators with an administrator account for performing system administration and a limited privilege account for performing non-system administration tasks.

Authentication and Authorization		
What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?
Shared systems or network accounts could lead to the disclosure of patient information to individuals who do not have a need-to-know even though they may be authorized individuals. Weak passwords can be easily guessed. If successfully guessed, health information could be viewed by unauthorized individuals thereby putting patients' privacy at risk. Sharing passwords among staff means that in the event of a security or privacy breach, it will be impossible to identify who is	 Assign unique user IDs and passwords to users of (operating) systems and network. Put strong password policy in place and enforce it. Develop, document and communicate a guideline to help users in selecting and securing passwords. Cover the guideline during security awareness training. This in an example of a strong password policy: Minimum length of 8 characters; Must include a combination of three of the following four: 	





actually responsible for the breach.	 alpha-upper case, alpha-lower case, numeric, or special characters; Passwords must not contain an individual's user name or full name; Must expire after 90 days; Minimum of 24 iterations before password reuse; 	
	Minimum of 24 iterations	
	lockout; • Minimum lockout duration of 30 minutes.	

	Internet Security Software			
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?	
1.8	The absence of an up-to-date Internet security suite leaves systems vulnerable to attack by computer viruses and other malicious codes. Viruses and malicious codes are used by attackers to steal, corrupt or delete data that could lead to loss of service, unauthorized modification and/or disclosure of health information.	 Install a licensed Internet security suite to ensure support from the vendor. Make sure that the security suite contains antivirus software. Configure the antivirus software to run automatic system and realtime scans on a regular basis. Configure the antivirus software to run automatic virus definition updates. Make sure the Internet security suite or software is regularly patched as appropriate. 		





		Firewall	
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?
1.9	Without a properly configured network-based firewall, an organization's network is opened to attacks. An attacker could use a hole in a firewall or the absence of a firewall to gain access to a clinic's network. There is a potential for health data to be stolen. Health data risks being viewed by unauthorized individuals. Legitimate users could be denied access to services and data leading to disruption of normal business operations.	 At a minimum, install a network-based firewall. Install or enable host-based firewalls on computers. Ensure that firewalls are properly configured such that undesired traffic is prevented from getting into or out of the internal network. Protect and prevent firewall configuration settings from being changed by unauthorized users. Regularly check firewalls to ensure they are working properly and appropriately. Regularly patch software-based firewalls using approved vendor patches. 	

		Patching	
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?
1.10	An unpatched system is vulnerable to attack. An attacker can exploit vulnerabilities in an unpatched system to gain access to the system or data stored in it or other systems connected to it. This access	 Develop, document and implement a consistent patch management process. Patch systems regularly. Apply critical patches as soon as they are released by the various vendors. Automatic update could be enabled 	





can be used by hackers or malicious software to steal or corrupt data. This could lead to unauthorized disclosure or modification of health information or cause data or clinical systems to be unavailable to legitimate users.

Threat and Risk Assessment			
What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?	
Without a comprehensive Threat and Risk Assessment (TRA), it will be difficult to identify all the major risks the systems and clinical applications are exposed to. Also, it will be difficult to determine whether current physical, administrative and technical security controls actually and appropriately protect health information.	 Perform a comprehensive TRA at least every two years and preferably annually so as to identify the risks on critical assets. Prioritize the risks on critical assets. Develop a mitigation plan to mitigate against the risks identified. Implement the mitigation strategies in the mitigation plan while prioritizing risks with high impact to the organization. As a check, perform a second TRA to ensure that the major risks identified during the first TRA have properly and appropriately been mitigated. If a technical assessment of the current network configuration was done during the development of a 		





PIA then the PIA could be used as a substitute for a TRA. The PIA that was accepted by the Office of the Information Privacy Commissioner must be less than two years old to meet the TRA requirement. As a reference for the TRA requirement, see the HIA practice guidelines and manual and the
COACH guidelines.

	Incident Response			
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?	
1.12	The absence of an appropriate and formal incident response process could lead to poor and inconsistent management of incidents that could aggravate rather than minimize the impact of an incidence. Also, there will be no records of past incidents and mitigation strategies that were implemented when they occurred. As a result similar security and privacy incidents may take longer to be resolved.	 Develop and document an incident response process that minimizes the probability and resulting damage of a security incident. Specifically address the incident identification process, who should be notified in the event of an incident, escalation procedures and corrective actions. Cover this process during security awareness and training. Document occurred incidents and the mitigation techniques that were used to address them for future reference. Update the incident response process document as appropriate. 		





Section Two: Mandatory Security Requirements for S2S Sites

Has a PIA been accepted by the Office of the Information Privacy	Yes No	
Commissioner (OIPC) and is it based on the current network configuration? If		
yes, state the date of acceptance.	(Double click box to check or uncheck)	į
	Acceptance Date:	
	ricceptance Date.	

	HIA Compliance			
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?	
2.1	If users are not assigned specific roles and are not well educated and trained about their responsibilities in relation to those roles under the Health Information Act (HIA), they can collect, access, use or disclose health information contrary to the act. They could access information that they do not have a need-to-know, not exercise least degree of anonymity during information disclosure and collect more data than is required to perform a given task.	 Clearly define and document the role for each user of health information. Provide user education for those roles as appropriate. Review and update user roles as appropriate. Incorp-ORAted user roles into clinical systems such that users have only those permissions that allow them to access just the information they need for their job tasks. 		





	Information Security Classification		
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?
2.2	If information is not properly classified, improper and weak security controls could be used to protect them. As these weak controls could easily be compromised, health information risks being viewed, modified, corrupted or deleted by unauthorized users. Patients' privacy and safety is at risk and normal business operations could be disrupted.	 Classify information into distinct groups such as restricted, confidential, protected, public use. For each classification level, apply appropriate set of security controls to protect the data. Perform a periodic audit to check or ensure that the security controls appropriately and adequately protect those information assets. Cover the information security classification scheme during security awareness training. 	

		Secure Storage	
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?
2.3	If master copies of software are stored within a facility equipped with inadequate or inappropriate physical and environmental security controls, they could be stolen or damaged by water, fire, or dust. These software copies risk not being available when needed to recover key business systems. This could lead to	 Store extra master copies of software in a facility separate from your business facility. Make sure that the storage facility has proper physical and environmental security controls (locked doors, fire extinguishers, temperature and humidity detectors, fire alarms, etc) in place. Review and test these controls 	





longer downtime in the event of		regularly to ensure that they	
an incident.		function properly.	
	•	Contract a reputable third party to	
		take care of your storage needs.	

Physical Security			
What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?	
If the server room does not have appropriate access controls in place, the server could be compromised or even stolen. Patient privacy could, therefore, be breached.	 Have a dedicated server room. Lock server room at all times. Allow only authorized individuals into the server room. Log and review access to server room. Take actions to correct problems detected. 		

	Access Log Review for Clinical Systems			
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?	
2.5	Without an appropriate formal log review process, abusive and unauthorized accesses to health information may go undetected. The privacy of patients risks being breached and health information could be modified by unauthorized individuals without being detected.	 Create and implement a well-defined and documented log review process. Regularly review access logs for clinical systems and take appropriate actions to correct issues detected. Provide awareness training on authorized access to health information. 		
		 Tie user access permission to user 		





		role.			
	Network Segregation				
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?		
2.6	If the network is not separated into trusted and untrusted segments, the implementation of security resources or controls may not be properly and appropriately maximized. As a result, security controls put in place to protect health information will be ineffective and inefficient. As this causes network to be exposed to attackers, health information risks being corrupted, viewed, deleted, stolen or modified by unauthorized individuals.	 Segregate network into trusted and untrusted zones by using appropriate security controls such as a firewall. Perform a threat and risk assessment to identify the risks on your trusted zone Use appropriate security controls to mitigate the risks identified. For reference and troubleshooting purposes, have a copy of the logical network diagram in place. 			

	Password File Encryption			
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?	
2.7	If a user gains access to a password file that is in clear text, passwords are likely to be stolen and used to gain access to the clinical systems. Proprietary algorithms used for encrypting password files could be easily broken since the strength of these algorithms is unknown and	 Encrypt password files using Alberta Health and Wellness approved cryptographic algorithm. Properly secure the encryption key if a one-way hash function is not used. Limit access to the encrypted password files. Review system logs and determine 		





therefore could be insecure. and block access attempts to Health information risks being password files. viewed or modified by Do not use proprietary algorithms unauthorized individuals or to encrypt password files as these stolen or corrupted. Patients' algorithms do not go through privacy could be breached and rigorous industry and academic patient safety becomes a testing. concern. Business operations could be interrupted.

	Inactivity Session Timeout			
	What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?	
2.8	The absence of an appropriate timeout for the clinical systems after a certain defined period of user inactivity leaves the clinical systems vulnerable to eavesdropping. In the event that an unauthorized user gain access to the operating system when the clinical systems did not timeout after prolong period of user inactivity, patient privacy could be breached. Depending on the permission of the clinical systems account, health information could be deleted, corrupted or stolen causing patient safety and privacy concerns.	 Conduct a Threat and Risk Assessment (TRA) to determine the risks that could be mitigated by configuring system timeout. Categorize timeouts as long, medium or short such that each timeout category mitigates a set of risks identified during the TRA and the exposure to such risks. Configure the clinical systems to appropriately time out after a defined period of user inactivity. Configure the operating system screen lock to be automatically activated after a specified period (less than the clinical system timeout period) of user inactivity as an additional layer of security. Create and enforce a policy to ensure that users log out of 		





	clinical systems or activate the operating system screen lock before leaving a workstation unattended. Cover this policy during security awareness training.
--	---

Password Standard for Clinical Systems		
What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?
Shared clinical systems accounts could lead to accidental disclosure of patient information to legitimate users who do not have need-to-know. Weak passwords can be easily compromised. When successfully compromised, health information would be viewed, modified or deleted by unauthorized individuals. Patients' privacy, data completeness, correctness, and availability are at risk.	 Assign unique user IDs and passwords to clinical systems users. Put a strong password policy in place and enforce it. Develop, document, communicate and maintain password guidelines to help users in selecting and securing passwords. Cover the guidelines during security awareness training. This is an example of a strong password policy: A minimum length of 8 characters. No embedded part of user's name, A combination of three of the following four: alpha-upper case, alpha-lower case, numeric, special characters, Validity password period of 90 days. 	





Remote Access		
What are the Risks?	What could be done to Mitigate the Risks?	What does your practice do?
If an insecure communication line is established during remote access to health data, there is a risk that the data 2.10 could be intercepted as it is being transmitted. This puts patient privacy and safety at risk. In addition, if passwords are not encrypted, they could be obtained by malicious users. They can then use them to get access to clinical systems which potentially put health information at risks of being breached.	 Follow a well designed, documented, enforced and maintained remote access policy for all remotes access to the provider's network. Cover the remote access policy during security awareness training. Implement AHW or GOA approved method of remote access such as key fob, Citrix, VPN, SSL. 	





Section Three: Wireless Security Assessment

Instructions: The requirements 1-13 are assessed upon initial setup. Any change in security policy, wireless hardware or network equipment must be reported to Alberta Health and Wellness (AHW).

	Implementation Tasks	Information needed	Compliance details
3.1	Purchase and use Access Points (AP) and switches that are 802.1X capable.	Provide Make and Model number of the AP and switches	
3.2	Develop an organizational security policy that addresses the use of wireless networks. Address usage of Bluetooth devices in the policy.	Confirm if security policy has been developed to address the use of wireless	
3.3	Has the default administrative login and/or password been changed? A new password must meet a good password standard such as AHW password standard. See section one for an example of a good password standard.	Provide status	
3.4	Locate AP in secured areas that are more central and away from exterior walls and windows. Usage of directional antennas to limit the stray signal is recommended.	Details on compliance	
3.5	Ensure AP channels are on different channels from any other nearby wireless networks to prevent interference.	Provide status	
3.6	Make sure the reset function on AP is being used only when needed and is only invoked by an authorized group of people. Tamper proof seal is recommended on the reset button.	Provide status	
3.7	Ensure that AP uses a unique non-	Provide status	





	identifiable SSID.		
3.8	Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to AP).	Provide status	
3.9	Ensure that the "ad hoc mode" for 802.11 has been disabled on all the client devices.	Provide status	
3.10	Disable all insecure and nonessential management protocols on the AP, such as SNMP.	Provide status	
3.11	Do not disable user authentication mechanisms for the management interfaces of the AP. Credentials for the management utilities should also not be cached on clients?	Provide status	
3.12	Enable WPA or WPA2 (preferred). Use a pass phrase on the access point, the pass phrase must comply with AHW password standard.	Provide status	
3.13	Document MAC addresses for all network devices. Use the documented list of MAC addresses to check for rogue devices. It is recommended to enable MAC filtering in the AP.	Provide Status	

Instructions: The requirements 14 -19 are to be assessed on **annual basis**. Custodians must ensure the following requirements are reassessed annually. Any changes require a wireless assessment to be resubmitted to AHW.

3.14	Perform comprehensive security assessments at regular intervals to locate	Provide how often security	
	any rogue AP, extent of wireless coverage and that AP are adhering to strong	assessments are performed or scheduled	
	password policy standards.		
3.15	Take a complete inventory of all AP and	Confirm the inventory of all	

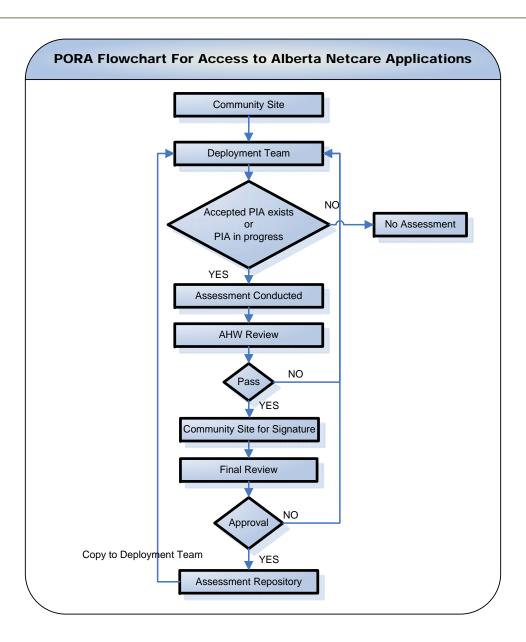




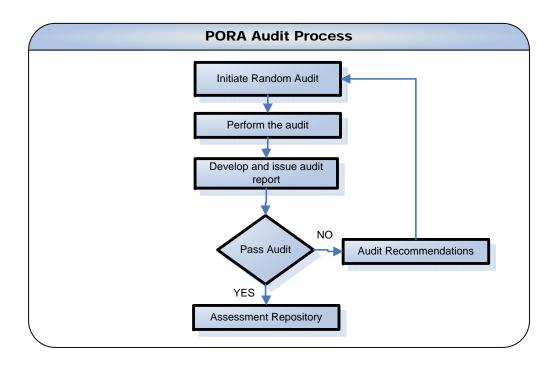
	802.11 wireless devices.	AP's and 802.11 wireless
		devices and provide
		schedule of the inventory.
3.16	Ensure users on the network are fully	Details on compliance and
	trained in computer security awareness and	ensure that wireless
	the risks associated with wireless	security awareness is part
	technology	of user induction process
3.17	Restore the AP to the latest security settings	Ensure that documented
	when the reset functions are used and that	procedure is changed to
	all default parameters are changed. In case	reflect the modified
	the reset button has been pressed,	security settings on AP
	documented procedure must be readily	
	available to ensure that the latest security	
	settings are in place.	
3.18	Default shared keys must be periodically	Provide schedule
	replaced by more secure unique keys	
3.19	Fully test and deploy software patches and	Details on compliance
	upgrades on AP on a regular basis as well	
	as firmware upgrades.	











AHW Confidential (when completed)

Version 1.1

Page 23 of 24





Review History

Version	Date Revised	Revisions	Reviewers			
1.0	April 1, 2008	Initial assessment document	AHW, HSSWG,			
	(released date)		OIPC, Deployment			
			Team			
1.1	June 4, 2008	• Cover page: Allocation made for the signatures of other Security Officers. A field added for "Remarks".	AHW			
		Frequently Asked Questions revised.				
		Question on wireless network included in the first section.				
1.1	July 8, 2008	Requirement 3.2 removed.	AHW			
		Requirement 3.3 added.				
		Requirements 3.12 and 3.13 updated.				



Alberta Netcare Access Administrator Reference Guide

Developed and maintained by:

Information Compliance and Access (ICA) Unit
Information Management Branch
Health System Performance and Information
Management Division



Health and Wellness

Table of Content

1	Purpose of Guide	3
2	Appointing an Access Administrator	3
3	Access Administrator Responsibilities	3
	Information Security Awareness	
5	Reporting Information Security Incidents or Problems	5
App	pendix A	7
Sect	tion 1: Netcare Access Administrator Registration Form	7
Sect	tion 2: Alberta Netcare Portal User Registration Form	9
Sect	tion 3: Role Assignments	11
App	pendix B	16
Inci	dent Reporting Form	16

Health and Wellness

Access Administration Guide

Purpose of Guide

This guide provides Access Administrators (AA's) with tools to assist them in successfully carrying out their responsibilities for managing Alberta Netcare Portal (ANP) users' permissions and providing appropriate support for access authorization.

Access Administrators can access copies of the latest forms on the ANP login page.

Appointing an Access Administrator

An Access Administrator (AA) is the primary contact with Alberta Health and Wellness (AHW) at a facility (or site). As such, this person is responsible for user registrations, amendments and deletions for access to Alberta Netcare via the ANP.

In Alberta Health Services (AHS) facilities or sites, AA's are approved by the AHS Executive Director, IT Security & Compliance and are acting on their behalf to ensure user access to confidential health information is properly administered and given only to those who need access to perform their jobs.

In community sites, like physician offices and pharmacies, AA's can be the custodian or a delegated representative responsible for liaising between the custodian(s) (see "Custodian Authorization Section of the AA Form) and AHW. The AA is responsible to ensure user access to confidential health information is properly administered and given only to those who need access to perform their jobs.

Access Administrator Responsibilities

ANP Registration and Access Control:

- Assist ANP users to complete user registration forms in their facility and submit the user registration requests in a timely manner.
- Periodically reviewing ANP access at the facility to ensure user's permission levels are still relevant to the job they perform and information is only accessed on a need to know basis.
- Submit user access termination requests as soon as the user no longer requires
- Comply with all statutory, regulatory and policy requirements to keep confidential any individually identifying information that is collected for user management process.
- Monitor and maintain the access control rules within the ANP that provide controlled access in accordance with defined information access requirements.
- Periodically review the ANP user list, users' permissions and contact information, and submit changes to user access as appropriate.
- Please see appendix A for more details regarding access level selection guide and permission matrix for ANP.

Information Security Awareness:

- Ensure users are trained about information security and privacy issues.
- Ensure users are trained about incident response process and how to report security and privacy breach. Please refer to section 4 for more details.

Reporting Information Security Incidents or Problems:

- Assist in investigation of potential information security or privacy breach in Alberta Netcare.
- Act as a liaison between AHW Information Compliance and Access Unit (ICAU) and the custodian to evaluate the effect of any changes on security and privacy controls.

AHW Protected V 2.0 Page 3 of 16

Health and Wellness

Access Administration Guide

Please refer to section 5 for more details.

4 Information Security Awareness

Access administrators are responsible to ensure that users protect Confidentiality, Integrity & Availability of health information. As custodians, health stakeholders are all accountable for protecting the confidentiality, integrity and availability of health information. Health Information is a valuable asset and is essential for the delivery of services and the development of policy decisions that are in the best interests of Albertans.

- Protecting the confidentiality of information means sharing sensitive or proprietary
 information with others only if you have been authorized to do so, and only if they have a
 need to know. It also means taking steps to prevent any unauthorized disclosure of
 information. E.g. granting access to health information to individuals that do not have a
 "need to know" causes loss of confidentiality.
- The **integrity** of information is about maintaining the reliability and accuracy of information so it can be used to make informed health decisions. An unauthorized change of health information used for decision making or an error in the information is an example of something that causes loss of integrity.
- Ensuring the continued **availability** of information means it is accessible to those who need the information when it is needed. A system outage is something that causes loss of availability.

All health information is classified as confidential based on the following Information Security Classification:

AHW has adopted Information Security Classification structure from the Government of Alberta. The government has developed an Information Security Classification guide that describes four information security classifications based on sensitivity to loss of confidentiality.

- Unrestricted information is not sensitive and includes information that can be routinely shared with the public including blank application forms, published news releases, fact sheets, public reports and policy statements.
- Protected information is considered sensitive if shared outside the organization, but is
 usually available within the organization to employees who need to know the information
 to do their job. Protected information can include draft versions of documents and some
 internal discussion papers intended to provide options for decision makers.
- Confidential information is sensitive even inside the organization and is accessible only
 to employees in specific functions or roles. All health information is classified as
 confidential.
- **Restricted** information is highly sensitive and only available to specific employees. This includes criminal investigation documentation and sensitive personal medical records.

Access to health information should be granted based on the following Health Information Act Security Principles:

• Need-to-Know: People should only have the minimum amount of health information that they need to know in order for them to perform their duties. Access to health information should only be granted if it is required for the job function the user is performing. From an administrative perspective, the Access Administrator should regularly review the kinds of health information that their ANP users have access to. The Health Information Act establishes the rules for how information may be collected, used and disclosed. Furthermore, it establishes the principles of respecting the highest degree of anonymity,

AHW Protected V 2.0 Page 4 of 16

Government of Alberta
Health and Wellness

using the least amount of information, based on a need to know that information. For further details on the Health Information Act, consult the HIA Guidelines and Practices Manual:

http://www.health.alberta.ca/documents/HIA-Guidelines-Practices-Manual.pdf

- **Segregation of Duties:** This means dividing job responsibilities for sensitive job functions between several individuals in order to provide a check and balance. For example, someone investigating a security or privacy incident should not be someone who was involved in the circumstances of the incident.
- Authorization to Use and Disclose: Once you have been given access to information, you are required to use that information only during the course of your work. Using or disclosing that information for personal gain or for purposes outside of the Health Information Act is prohibited. The Health Information Act sets out fines for custodians and affiliates who knowingly breach the Act.

For further information regarding the *Health Information Act*, please contact the HIA Helpdesk at **780-427-8089** or by email at **hiahelpdesk@gov.ab.ca**.

Custodians and access administrators are responsible for ensuring that their affiliates are aware of safe electronic and physical document handling.

There are some general guidelines that should be followed to keep health information secure.

- Ensure that information (e.g. medical record) is not visible to others whether it is on the workstation or on the desk.
- Verify that an e-mail address or fax number is correct before sending information.
- Lock the computer workstation at all times when not in use. (Press Control-Alt-Delete)
- Ensure that users understand it is their responsibility to ensure that health information is
 only shared based on a "need to know" principle. If not sure, it is better to be cautious
 and ask their supervisor or consult with the access administrator.
- Ensure access to areas where information is processed or stored is controlled and restricted to authorized persons only.

5 Reporting Information Security Incidents or Problems

An information security incident occurs when there is a violation of the *Health Information Act* or a violation of your organization's security policies or when there is a failure or absence of required safeguards providing for the loss of confidentiality, integrity or availability.

Some examples of security incidents include:

- A missing laptop, PDA or portable storage device containing health information
- Virus, spyware or malware infection impacting health information
- Disclosure of passwords or other authentication credentials associated with ANP
- Error in patient's profile in ANP

Health stakeholders can use their local incident management process in their organization to manage their internal incidents. AHW can be consulted for breaches of health information, to ensure appropriate actions are considered.

All suspected incidents for Alberta Netcare must be reported using the incident reporting form located on ANP login page, sample form is found in Appendix B.

The defined Provincial Reportable Incident Response Process (PRIRP) will be followed to respond to the suspected security and privacy incident. The Provincial Reportable Incident Response Process (PRIRP) has been designed to ensure that all health

AHW Protected V 2.0 Page 5 of 16



stakeholders such as community custodians, Alberta Health Services and health service partners are appropriately involved to respond to a suspected or real threat.

If you have any questions or prefer to report an incident by phone call the EHR Helpdesk at **1.877.931.1638** or **780.412.6778** or contact the HIA Helpdesk at **780-427-8089**; or complete the form located on ANP login page and email it to ahw.security@gov.ab.ca.

Linked Documents and Items

Name	Owner	Location			
Netcare User Registration Form V3.1	AHW	ANP login page			
Netcare Access Administrator Form	AHW	ANP login page			
Incident Reporting form	AHW	ANP login page			

Versions

Version	Date	Revisions	Reviewers
2.0	April 2010	Revised the Access Administrator V1.5 guide	ICA Unit

AHW Protected V 2.0 Page 6 of 16

Access Administrator

Appendix A

Section 1: Netcare Access Administrator Registration Form



Access Administration Registration

Note: Individually identifying information that is collected will be used for the creation/amendment/deletion of an Access Administrator. It will be subjected to statutory or regulatory requirements, and kept confidential by Alberta Health and Wellness. This form is used to setup an Access Administrator who will then be responsible for user setup at the same facility. This form is also used to create facility permission for the application(s) being accessed, if facility permission has not already been created. Please print clearly to ensure correct verification of information.

Alberta Netcare Transition Coordinator/

Contact for this Site Implementation:

Please check one of the following:	Create Access	Adminis	trator	Access Administrator (<u>piease ur</u>	nderline am	nendments)	□ Delete	Access A	Adminis	trator		
Organization Name (name of health regio	n, physicians of	fice, or lic	ensed pharmacy)									
Facility Name Site Name (i.e. Admitting)		Fadility ID Number	Name of Health Region where facility is located									
Facility Type			L	Primary Service Type				Other/Additional Service Types				
Select One Active Treatment Clinic Active Treatment Hospital Ambulatory Care Centre Auxillary Hospital Blood Bank Community Pharmacy Diagnostic Clinic Federal Institution (other than Jail) In-Patient Pharmacy Lab Collection Medi-Clinic Mental Health Regional Clinic Mobile Clinic Site Mailing Address	e e. (Medical) e. (Non-Medical) ab ent Centre e dministration	Select One Anesthetic Consultation Diagnostic Services Eye Glasses or Dental Services Office Visit (s) Other Pharmacist Professional Procedures/Surgery Surgical Assists Surgical Services X-Rays		Select one or more, if applicable Anesthetic Consultation Diagnostic Services Eye Glasses or Dental Service Office Visit (s) Other								
City		Provin				Postal co	do					
			vince					I				
Access Administrators Surname		First N	ame		Middle Name							
Date of Birth (for unique identification only Day Only Mor	Phone (hone)			Fax ()							
E-mail												
Secret Word (for caller verification with he	elp desk)			Prompt								
A Secret Word will have meaning to Note: Access Administrator must con Custodian Authorization				r memory for your secret w	ord (e.g.	mother's r	maiden nar	ne).				
Note: All Access Administrator approvals For health regions: VP level or above; for multiple physician custodians appoint on I hereby authorize the creation, amendme	physician office Access Adminis	s: Physic trator, all	ian custodian under physicians are requ	HIA; for pharmacles: Pharma						form.		
Full Name				Position								
Signature Date Day Month Yes							Year					
Phone	Phone Fax E-mail											
()	()											
Figure 1 – Alberta Ne	etcare Po	ortal	2006 Acc	ess Administrat	or Re	aistra	tion F	orm				

AHW Protected V 2.0 Page 7 of 16

Health and Wellness

Access Administrator Registration form required to be completed for:

- Creation/amendment/deletion of an Access Administrator at a facility (or site).
- A change in the *Health Information Act* custodian.
- An amendment/deletion of an organization name, a facility/site name, or a site address.

Access Administrator section of the Form:

Organization Name: It is the **legal name** of your health organization (e.g. AHS sites name, physician office name or licensed pharmacy name). This is the name that should be registered with AHW. Any changes to an Organization Name should be updated with AHW using a Facility Registration Form.

The Facility and Site Name: The facility name is the name of a building or building complex at one specific address registered by the authorizing custodian with AHW. It is the physical location of an organization. e.g., ABC Hospital, ABC Medical Clinic, or ABC licensed pharmacy. Within a facility, there is at least one site associated with that facility. A site is used to identify where a patient encounter with a health stakeholder occurs. There could be multiple sites within a facility like a hospital (e.g., Admitting, Emergency, Lab, etc.) that could have their own site identification code.

The *Health Information Act* defines 'affiliates' of Custodians and states that all affiliates are accountable to the Custodian and also accountable in their own right. Consequently, it is up to the custodian to identify and request any affiliate sites, (e.g., labs they have agreements with), if the lab staff require access to ANP.

Facility ID Number: The Facility ID Number is a unique facility identifier assigned and managed by AHW. These are provided to the custodian by AHW.

Health Region Name: Used to identify a Health Region prior to April 1, 2009. The default for this is now AHS.

Secret Word: A secret word is a word that has special meaning **only** to the Access Administrator. It is required for caller verification when the Access Administrator calls the help desk (1 877 931 1638), so it should be a word the Access Administrator can easily remember.

Prompt: If an AA forgets the secret word, which is required for caller verification with the help desk (1 877 931 1638), the help desk will provide the prompt. (e.g., Secret word: Smith. Prompt: mother's maiden name)

Custodian Authorization section of the form:

Who signs the Custodian Authorization section?

- For AHS: At minimum AHS Executive Director, IT Security & Compliance.
- For physician offices: in a single physician office, the physician; in a multiple
 physician office, ALL physician custodians are required to sign the form. Page 3 of
 the Access Administrator Form provides additional space for physician signatures in
 large physician offices.
- For pharmacies: the pharmacy licensee whose name is registered with the Alberta Pharmaceutical Association.
- For AHW: AHW Privacy Manager

AHW Protected V 2.0 Page 8 of 16

Section 2: Alberta Netcare Portal User Registration Form

Netcare V			Albe	rta Net	care	Porta	al User	Regist	ration		Version 3.01		
User Information Se	ection (To	be com				tion Coordinator / Contact:							
Please check one of the following:			Create User		☐ Amend U		Jser	☐ Delete User (F		leturn fob)	☐ Name Change		
Title (E.g. Dr., Last Name						Legal Fi	rst Name	_		Middle Name			
Previous Surname			Pi	referred Fir	st Name								
(For Name Change Only) Date of Birth (for unique is	dentification	only)		Gender		Mothe	r's Maiden	Name					
Day Only	Month On	-		☐ Femal	e								
Profession				male		Professional ID (Assigned by Professional Regulatory Body e.g. License #)							
Business Address						City / Province Postal Code							
Business Phone	F.	ax			E-mail Address								
Secret Word - a word that caller verification with the l										Desk to help you mendment / dek	recall your Secret etion.		
Is Remote Fob Access req				dy have a r V applicatio		ccess	ss If Yes, note Serial Number of Token				access from		
Yes No			□ No	• аррікаци			OI TOKEII			□PC	☐ MAC ☐ Both		
Access Authorizer				cility ID/DP	HI Site I	D			Health R	gion			
(To be filled out ONLY by the Ao	oess Authorize	1)	Facility I	Name					Site Type Community Health Region Facility				
Select only one of the	he followi lete Facility	ing:	Site Nan	ne (e.g. Ad	(e.g. Admitting)				Comments				
☐ Change Facility			Old Facil	ity (ID/Nam	e):				New Facility (ID/Name):				
☐ Portal 2006 Acce	ess Inforn	nation	(Final p	ermissions	assign	signed to user)							
Permission Matrix User for to assign this User (Check ONE only)	Clini		1 [1 [1 [2 🗆 :	3 🗌 4	5 5 5 5 5	6 0 (CH Only) 7 [8 🗆	9 10			
☐ System to Syste	m Acces	s (CI	eck only	one PIN pe	rmissio	n box)] Amend §	S2S access	Dele	te S2S access		
☐ View PD (required)	PINI	.ook-up		PIN Preso	ribe	☐ PIN	Delegate fo	or Physician					
☐ Person Directory	(PD) Ac								permissio	n box.)			
☐ View PD ☐ Vie only Upd	w and ate PD		View PI Newbor	0 including n			Update PD Newborn		Amend P	D access	Delete PD access		
☐ Pharmaceutical	Informati	on Ne	twork (F	PIN) Acce	ess Lev	vel (F	PIN isacli	nical applic	ation - Che	eck only one pe	ermission box)		
☐ PIN Look up ☐ PIN Dispense (Pham	naciete Only	Pogu	ired for ac	Idina		PIN Presi		cord Prescri	ntions for		Amend PIN access		
allergies and intolerances)		- Requ	illed for ac	iding	Phys	,	galeu to Re	coru Frescri	ptions for		Delete PIN access		
□ Pharmacy Batch	Access ((Retail	Pharmaci	es Only)	☐ Ad	ld acces	s to Pharm	acy Batch		Delete access	to Pharmacy Batch		
☐ Delete Portal 200	Mont	Month Year Fob Returned: ☐ Yes ☐ No					s □ No						
Authorizer Name – Please Print (For Health Regions Only)						Authorizer Signature (For Health Regions Only)							
I am an authorized Ac	-	inistra	tor for t	he facility	v and s					the creation.	amendment or		
deletion of this User I													
First Name Initial Facility / Health Region Business Phone							ast Name	Day	Т	Month	Year		
Title					Signat	ture / Initi	als	Juj					
Transition Coordinator's Si	ignature / Da	ite											
	Complet	ed Use								rdinator or			
faxed	to the Alb	erta Ne	etcare De	ployment	t Team	office a	t: (780)6	41-1003 oı	r RHA at _				

Figure 2 – Alberta Netcare Portal User Registration Form

Alberta Health and Wellness Confidential (When Complete)

AHW Protected V 2.0 Page 9 of 16

Government of Alberta

Health and Wellness

ANP User Registration form is to be completed by each individual requesting to access or amend access to Alberta Netcare via the ANP.

- Users who require access to Alberta Netcare Portal from more than one site (e.g. physician office, pharmacy or AHS) need to complete more than one user registration form.
- Each form is signed by the AA responsible for user administration at each facility/site.

ANP User Information Section:

All ANP users must check one of the following boxes: Create User, Amend User, Delete User and Name Change. The approval office to which the user reports must authorize access to ANP by signing the Alberta Netcare Portal User Registration form

Create User: To be checked if user has not previously had an ANP account. All fields are mandatory, except where not available e.g. email address.

Amend User: To be checked if user has previously had an ANP account and requires a change in access, facility, secret word or prompt, department, authorizer or permission. All fields are mandatory, except where not available e.g. email address.

Delete User: To be checked if a user terminates employment or transfers to another facility, the outgoing approval office to which the user reports must authorize the disabling of Netcare access by signing the User Registration form. Mandatory fields – Surname, Legal First Name, Middle Initial, Preferred Name (if used), DOB to uniquely identify user, Facility Name, Authorizer Name, Authorizer Signature, AA Name, AA Signature

Name Change: To be checked if the user's Surname has changed. Mandatory fields – Last name, Previous Last Name, Legal First Name, Middle Initial, Preferred Name (if used), DOB – to uniquely identify user, Authorizer Name, Authorizer Signature, AA Name, AA Signature

Secret Word and Prompt: The Secret Word and Prompt are required for identity verification when a user calls for assistance.

Remote FOB access: If remote access is required, each remote user requires a remote access Token (fob). If the user already has a remote access Token from AHS or from AHW, provide the Serial Number recorded on the back as requested. Existing Tokens can be used for access to Alberta Netcare, via ANP.

Access Authorizer and Access Administrator section:

Facility ID Number: The Facility ID Number is a unique facility identifier assigned and managed by AHW. These are provided to the custodian by AHW

Facility and Site Name: The name of the facility and site as identified on the AA Form.

Portal Access Information: Check <u>ONE</u> Permission Matrix User Role based on the User Group Work Flow and Permission Matrix found in Appendix A of this Guide. It will guide you through a simple question process to determine the User Group a user should be assigned to.

Person Directory (PD) Access Level: check only <u>ONE</u> box and check the applicable PD permission box if the permission level differs from the default permission associated with the Role selected.

Pharmaceutical Information Network (PIN) access level: check only <u>ONE</u> box and check the applicable permission box if the permission level differs from the default permission associated with the Role selected.

AHW Protected V 2.0 Page 10 of 16



Authorizer Name and Signature (For AHS Only): Name and signature of person authorizing access for Alberta Netcare via the ANP. By signing the form, the person responsible for approval indicates agreement that this user performs the role and requires access to the health information selected.

As long as the approver maintains their authority as an authorizer, that person is also accountable for submitting an amend/delete if the user they authorized changes position or leaves. Until such notification is received, the authorizer is still accountable for actions carried out within Alberta Netcare Portal by the user they have authorized.

Section 3: Role Assignments

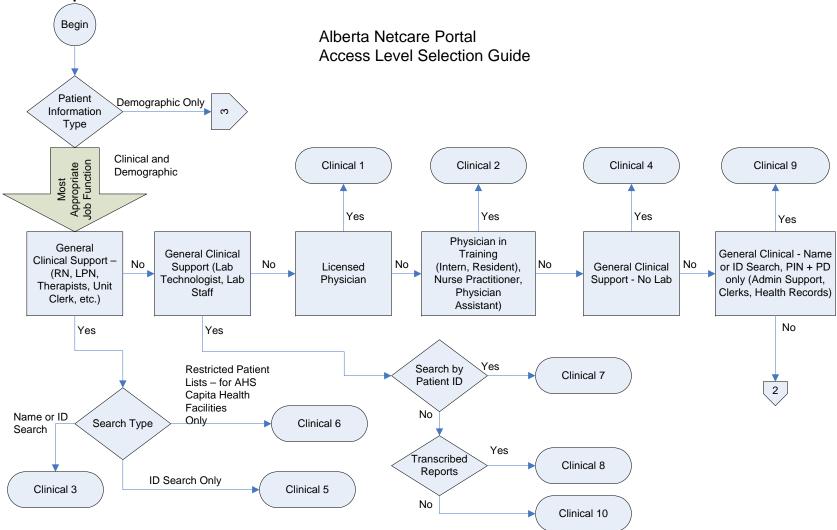
The following flow chart is provided as a guideline to assist AA's with assigning an appropriate user role based on the permission matrix.

Please refer to the Access Level Selection guide and Permission Matrix for further information to assign appropriate permissions to a user.

AHW Protected V 2.0 Page 11 of 16

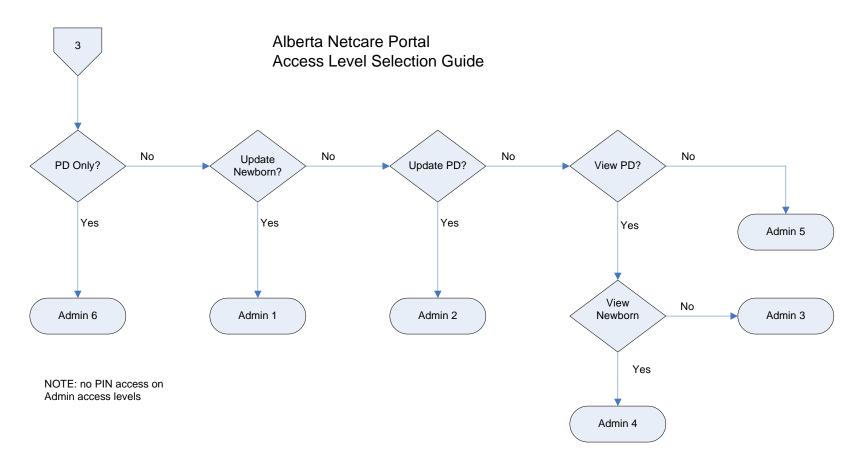


User Group Workflow Continued:



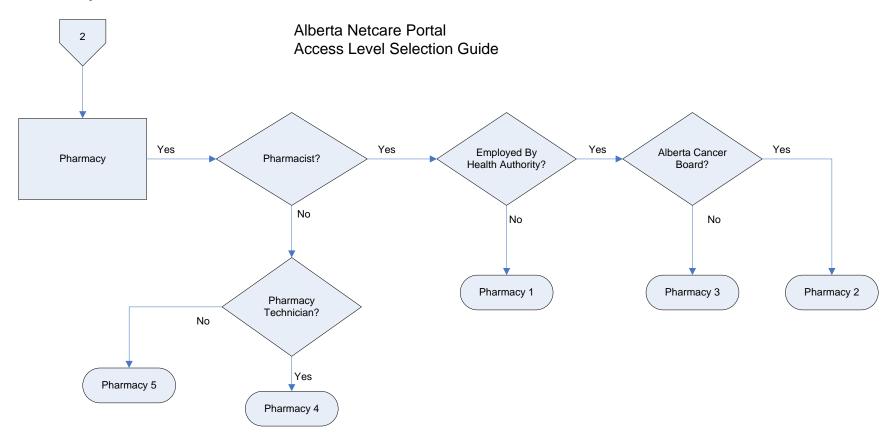


User Group Workflow Continued:





User Group Workflow Continued:





Administration Guide

Permissions Matrix:

		\perp												_			4			Щ	Щ	Щ.	Щ
						P	10	tal	ı						PII	N		ı	PD		ì	CH by	1
User Role	Description	Demographics	Patient Search	Patient Lists	Comment patient Control Restricted Patient Lists	Favorites	Access PD	Access PIN	Document Forwarding	Messaging	Event & Immunization Historu	Transcribed Reports	Clinical Documents	View	Prescribe	Prescribe Delegate	Uispense	View FU	Update Newborn	View Newborn			eSignature
Administra	Functions Supported	î												Ĺ			1						
Admin 1	Full Demographics, PD, Update Inc. Newborn - Health Records	Υ	Y	\top	т	ΙY	Υ	N	\neg	_	т	т	т	N	N	N I	ΝÌ	γŊ	7 Y	Y	\Box	\Box	
Admin 2	Full Demographics, PD View/Update - Health Records	Ý	Ý	_		Ý	_			1		+							ŹΝ		П	П	П
Admin 3	Full Demographics, PD View - Admitting Clerk	Y	Y			Y	_												N N			\Box	
Admin 4	Full Demographics, PD View Inc. Newborn - Admitting Clerk	Υ		\top	\top	Υ	Υ	N	\neg	\top	\top	\top	Т						4 N		П	П	П
Admin 5	Identifier Search, Concerto Only	Υ		١	Υ	Υ	N	Ν				T							N N		\Box	П	
Admin 6	PD Only - Billing Clerk	П	П	\top	T	Т	Υ	Ν	\neg	T	T	Т	Т	N	N	N I	ΝĪ	VT.	\top	П	П	П	П
Clinical	Typical Member					Т						Т		Г	П	T	T	T	T		П	П	
Clinical 1	Physician, IMG Physician	Υ	Υ	*	Т	Υ	Υ	Υ	Υ	ΥĪ	YΝ	7 Y	ΊY	Г	Υ	T	1	Υ	Т	П	*	*	*
Clinical 2	Fellow, Medical Resident, Nurse Practitioner, Medical Intern, Physician Assistant	Υ	Υ	*	Т	Υ	Υ	Υ	Υ	Υľ	YΝ	7 Y	ΊY	Υ	Π	Y	Ŧ	Υ	\top	\Box	*	*	*
Clinical 3	General Clinical - Name or ID Search	Υ	Υ	*		Υ	Υ	Υ	Υ	Υľ	YΝ	7 Y	ΊΥ	Υ	П		1	Υ			*	*	*
Clinical 4	General Clinical - Name or ID Search, no Lab	Υ	Υ	*		Υ	Υ	Υ	Υ	Υ	Y	/ Y	ΊΥ	Υ			Ţ	Υ	\perp		*	*	*
Clinical 5	General Clinical - ID Search by ULI or MRN	Υ		`	Υ	Υ	N	Υ	Υ	Υľ	YΣ	/ Y	'Υ	Υ					۱N		*	*	*
Clinical 6	General Clinical - access from patient list only - Capital Health only	Υ			Υ	·	N	Υ	Υ	Υ)	YΝ	/ Y		Υ	Ш				N N		ш	ш	*
Clinical 7	General Clinical - ID Search, Lab, Transcribed Reports	Υ		`	Y	Υ	N	Ν	<u> </u>	<u>Y '</u>	Y L	Υ			N	1 N			N N	N	\perp	*	*
Clinical 8	General Clinical - Name or ID Search, PIN, PD, Lab, Transcribed Reports		Υ	*	\perp	Υ	÷	Υ	Υ	Υ)	Y	Υ	'Υ	Υ	Ш	\perp		ΥY	4	Ш	\vdash	*	*
Clinical 9	General Clinical - Name or ID Search, PIN + PD_only (Admin Support, Clerks, Health	Υ		\perp	\perp	Υ		Υ		Y	\perp	┸	┸	Υ	Ш	\perp		Y	\perp	Ш			*
Clinical 10	General Clinical - Name or ID Search, PIN, PD, Lab Only	Υ	Υ	*	\perp	Υ	Υ	Υ	Υ	Υ)	<u> </u>	\perp	Y	Υ	Ц	\perp		YΥ	4	Ш	*	*	*
Pharmacy	Typical Member													L		\perp							
Pharmacy 1	Pharmacist - Name or ID Search, no Event History or Transcribed Reports (Community)	Υ		*		Υ	-	Υ		Υ!	-	\perp		Υ	Ш		ΥV					*	*
Pharmacy 2	Pharmacist - Name or ID Search (Cancer Board)	Υ	Υ	*		_	Υ	$\overline{}$	_	_	YΣ	_	'Υ	-	Ш		ΥV		\perp	ot	*	*	*
	Pharmacist - Search by ID (Hospital)	Υ		,	Υ	_	N	_	$\overline{}$	_	YΣ	<u> </u>	ΊΥ	÷		,			N N	N			
	Pharmacy Technician - Name or ID Search, no Event History or Transcribed Reports	Υ		*		Υ	_	Υ	_	Υ)	Y		Υ	•	Ш	\perp		Υ	\perp	\sqcup	\vdash	ш	*
Pharmacy 5	Pharmacy Staff - Name or ID Search, no Lab, Event History or Transcribed Reports	Υ	30	*		ΙV	lγ	\vee	V.	100				Ιv				VΕ			*	*	*





Appendix B

Incident Reporting Form

Government of Alberta Health and Wellness

Privacy and Security Incident Reporting

Purpose

To allow individuals to report Privacy and Security incidents or suspected incidents so that AHW responsibilities related to the protection of privacy and security are fulfilled, and to assist AHW in determining the cause of the actual or suspected incidents so that necessary changes are made to prevent future occurrences.

If you have any questions or prefer to report an incident by phone call *EHR Helpdesk at 1.877.931.1638* or 780.412.6778 or contact the ICA Unit at 780-427-8089; or complete this form and email it to ahw.security@gov.ab.ca.

Subject to any overriding legal obligations, all information on this form is protected. You may be contacted by the Information Compliance and Access (ICA) Unit during Incidence Reponse.

Incident Informatio	n												
Incidence Reference n	umber	Incident name			Inciden	t Short De							
Incident Initially detec	ted By:				e/Time I urred	ncident	Program/	gram/ Business Area Affected					
Asset Affected	Affected Number of Individua			duals			to this incident b area (High, Medio						
Incident Contact P	erson (f	or communic	cation a	nd fo	llow-uj	ps)							
Name	Job Titl	e	Phone			Fax	E-mail						
Incident Details													
Immediate Inciden	Mitiga	tion											
Additional Comme	nts/Note	es .											

								Por	tal								PIN		I	F	D		-	H - b	,
User Role	Description	Demographics	Patient Search	Patient Lists	Limited patient Search	Restricted Patient Lists	Favorites	Access PD	Access PIN	Document Forwarding	Messaging	Lab	Event & Immunization History	Transcribed Reports	Clinical Documents	View	Prescribe Prescribe Delegate		Dispense View PD	Update PD	Update Newborn	View Newborn	SDM	SMT	eSignature
Administration	Functions Supported																								
Admin 1	Full Demographics, PD, Update Inc. Newborn - Health Records	Υ	Υ				Υ	Υ	N		Υ				Ν					Υ	Υ	Υ			
Admin 2	Full Demographics, PD View/Update - Health Records	Υ	Υ				Υ	Υ	Ν		Υ				Ν			_	_	•					
Admin 3	Full Demographics, PD View - Admitting Clerk	Υ	Υ				Υ	Υ	N		Υ				Ν	_									
Admin 4	Full Demographics, PD View Inc. Newborn - Admitting Clerk	Υ	Υ				Υ	Υ	N		Υ				Ν										
Admin 5	Identifier Search, Concerto Only	Υ			Υ		Υ	N	N		Υ				Ν						N	N			
Admin 6	PD Only - Billing Clerk							Υ	Ν		Υ				٨	1 N	N	N	Υ	\bot					
Clinical	Typical Member																								
Clinical 1	Physician, IMG Physician	Υ	Υ	*			Υ	Υ	Υ	Υ	Υ			Ϋ́		Y			Υ				*	*	*
Clinical 2	Fellow, Medical Resident, Nurse Practitioner, Medical Intern, Physician Assistant	Υ	Υ	*			Υ	Υ	Υ	Υ	•	•		Ϋ́			Y		Υ				*	*	*
Clinical 3	General Clinical - Name or ID Search	Υ	Υ	*			Υ	Υ	Υ	Υ	Υ			Ϋ́	_				Υ				*	*	*
Clinical 4	General Clinical - Name or ID Search, no Lab	Υ	Υ	*			Υ	Υ	Υ	Υ	Υ			Ϋ́					Υ				*	*	*
Clinical 5	General Clinical - ID Search by ULI or MRN	Υ			Υ		Υ	Ν	Υ	Υ	Υ			Υ `	/ Y				N			N	*	*	*
Clinical 6	General Clinical - access from patient list only - Capital Health only	Υ				Υ		Ν	Υ	Υ	•			Ϋ́					Ν			Ν	*	*	*
Clinical 7	General Clinical - ID Search, Lab, Transcribed Reports	Υ			Υ		Υ	N	N	Υ		Υ		Υ `			N	N			N	N	*	*	*
Clinical 8	General Clinical - Name or ID Search, PIN, PD, Lab, Transcribed Reports	Υ	Υ	*			Υ	Υ	Υ	Υ		Υ		Υ `				┸	Υ				*	*	*
Clinical 9	General Clinical - Name or ID Search, PIN + PD only (Admin Support, Clerks, Health Records)	Υ	Υ				Υ	Υ	Υ		Υ				Y				Υ				*	*	*
Clinical 10	General Clinical - Name or ID Search, PIN, PD, Lab Only	Υ	Υ	*			Υ	Υ	Υ	Υ	Υ	Υ		`	′ Y	<u>′ </u>		丄	Υ	Υ			*	*	*
Pharmacy	Typical Member																								
Pharmacy 1	Pharmacist - Name or ID Search, no Event History or Transcribed Reports (Community)	Υ	Υ	*			Υ	Υ	Υ	Υ	Υ	Υ		`				Υ					*	*	*
Pharmacy 2	Pharmacist - Name or ID Search (Cancer Board)	Υ	Υ	*			Υ	Υ	Υ	Υ	•	•		Ϋ́				Υ					*	*	*
Pharmacy 3	Pharmacist - Search by ID (Hospital)	Υ			Υ		Υ	Ν	Υ	Υ	Υ		Y '	Ϋ́				Υ			N	N			
Pharmacy 4	Pharmacy Technician - Name or ID Search, no Event History or Transcribed Reports	Υ	Υ	*			Υ	Υ	Υ	Υ		Υ		`					Υ				*	*	*
Pharmacy 5	Pharmacy Staff - Name or ID Search, no Lab, Event History or Transcribed Reports	Υ	Υ	*			Υ	Υ	Υ	Υ	Υ				Υ	′			Υ				*	*	*

^{* -} Capital Health Region only, when appropriate forms are completed and signed by approved authorized

Y - standard access components

N - PIN/PD access component not available

blank - Portal access component not available

blank - PIN/PD access optional on a need to know basis

Access Administration Registration



Note: Individually identifying information that is collected will be used for the creation/amendment/deletion of an Access Administrator. It will be subjected to statutory or regulatory requirements, and kept confidential by Alberta Health and Wellness. This form is used to setup an Access Administrator who will then be responsible for user setup at the same facility. This form is also used to create facility permission for the application(s) being accessed, if facility permission has not already been created. Please print clearly to ensure correct verification of information.

Access Administrator			Alberta Netcare Transition Contact for this Site Imp				
Please check one of the following: Creat	ate Access Admin	strator	Access Administrator (<u>please</u>	underline amend	dments)	☐ Delete Acce	ss Administrator
Organization Name (name of health region, phys	rsicians office, or l	icensed pharmacy)					-
Facility Name		Facility ID Number	er	Name of Hea	alth Regi	ion where facility	is located
Site Name (i.e. Admitting)							
Active Treatment Hospital Ambulance Ambulatory Care Centre Auxillary Hospital Blood Bank	Nursing Home Other Penal Institution Pharmacy Practitioner's Off Practitioner's Off	ce. (Medical)	Primary Service Type Select One Anesthetic Consultation Diagnostic Services Eye Glasses or Dental Office Visit (s) Other Pharmacist Profession	Service C	Select one Anest Consu Diagn Eye G Office Other	ultation nostic Services Blasses or Dental e Visit (s)	cable Service
□ Diagnostic Clinic □ □ Federal Institution (other than Jail) □ □ In-Patient Pharmacy □ □ Lab Collection □ □ Medi-Clinic □ □ Mental Health Regional Clinic □	Provincial Health Public Health Un Public Lodge Recovery Treatm Red Cross Senior's Residen	al Health Lab Procedures/Surgery Procedures/Surgery lealth Unit Surgical Assists Surgical Assists y Treatment Centre Surgical Services X-Rays Surgical Services X-Rays					
City	Provi	nce		P	Postal cod	de	
Access Administrators Surname	First I	Name		N	/liddle Na	ame	
Date of Birth (for unique identification only) Day Only Month Only	Phone)		F	ax		
E-mail	()		()		
Secret Word (for caller verification with help desi	sk)		Prompt				
A Secret Word will have meaning to you (e	e.g. Smith). A	Prompt will jog you	ur memory for your secret	word (e.g. mo	other's n	maiden name).	
Note: Access Administrator must complete	e and sign page	two of this form.					
Custodian Authorization Note: All Access Administrator approvals need to	to come from Vice	President (VP) Leve	el or above				
For health regions: VP level or above; for physic multiple physician custodians appoint on Access I hereby authorize the creation, amendment or d Full Name	cian offices: Physi s Administrator, a	cian custodian unde Il physicians are requ	r HIA; for pharmacies: Pharr				
Signature						Date	
ogrado							lonth Year
Phone	Fax		E-mail				
()	()						
Please fax or mail this completed Acc Attention: Alberta Netcare Deployme							'80-641-1003
Processing - Alberta Health and Wellne	ess AH&V	V or Deployment T	eam Signature/Initial:	Date Day		Month	Year



Access Administration Agreement

Please read the Access Administrator Agreement and sign below

- 1. As an Access Administrator requesting creation/amendment/deletion of Alberta Health and Wellness Applications users, I agree to:
- 2. Assist application users to complete their forms, as required.
- 3. Collect and retain completed forms.
- 4. Submit all forms as soon as possible.
- 5. Comply with all statutory, regulatory and policy requirements to keep confidential any individually identifying information made available to me as Access Administrator.
- 6. Delete any application users who no longer need access to the Alberta Health and Wellness application and send the completed form to:

Alberta Netcare Deployment Team 44 Capital Blvd., 400 - 10044 – 108 Street, Edmonton, AB T5J 3S7 Fax: 780-641-1003

7. Send All fobs received from Alberta Health and Wellness to the users and return all fobs collected from the users to:

Alberta Netcare Deployment Team 44 Capital Blvd., 400 - 10044 - 108 Street, Edmonton, AB T5J 3S7 Fax: 780-641-1003

8. Immediately notify the Alberta Netcare Deployment Team if my responsibilities no longer require me to be an Access Administrator.

Unauthorized disclosure of individually identifying information obtained through the Alberta Health and Wellness application(s) may result in:

- penalties as described in relevant legislation;
- disciplinary action;
- termination of your ability access application(s);
- termination of your ability to authorize users to access the application;
- notification to the relevant professional regulatory authorities of any inappropriate use.

I agree to be an Access Administrator for Alberta Health and Wellness applications, and I understand and agree to comply with above terms and conditions.

Name				
	Day	Monti	n Yea	r
Signature	Date			
Initials				



Access Administration Registration

Access Administration Surname	First	Name		Middle Name)		
Custodian Authorization							
For health regions: VP level or above; for clinics, where multiple physician custodia please use page three of this form.							
I hereby authorize the creation, amendme Full Name	ent or deletion of Access Ac	dministrator.			Position		
Signature					Date		
O.g. initial of					Day	Month	Year
E II N					<u> </u>		
Full Name					Position		
Signature					Date Day	Month	Year
Full Name					Position		
Signature					Date Day	Month	Year
Full Name					Position		
Signature					Date Day	Month	Year
Full Name					Position		
Signature					Date Day	Month	Year
					,		
Full Name					Position		
Signature					Date Day	Month	Year
Full Name					Position		
Signature					Date Day	Month	Year
				L			
Phone	Fax	E-	mail				
()] ()						
Please fax or mail this completed Act Attention: Alberta Netcare Deployment						x: 780-6 4	1-1003
Processing - Alberta Health and Wellne	ess AH&W or Deploy	ment Team Signatu	re/Initial:	Date Day	Month	l Yea	ır

FAQs for Global Person-Level Masking

These FAQs will be formatted according to the learning Centre standard. This file is strictly for content review and signoff.

Source content for the FAQs:

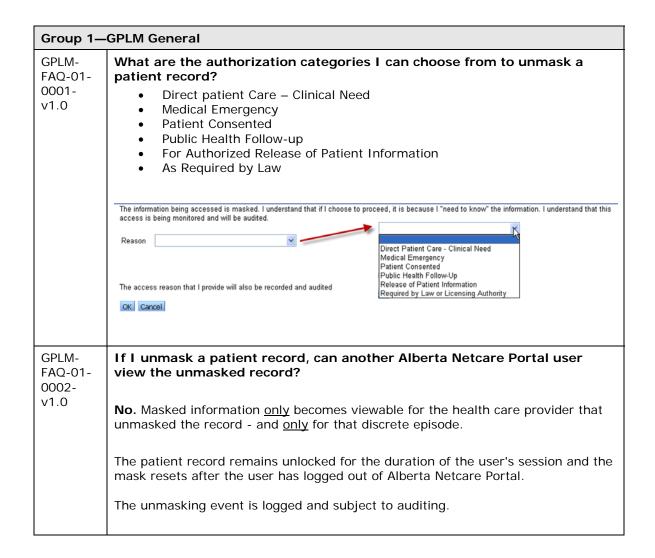
- Application for Global Person-Level Masking form, Sept 1 2008, v1.0
- Authorization to Rescind Global Person-Level Masking form, Sept 1 2008, v1.0

Group 1 - GPLM General

Group 2 - Applying or Rescinding a Mask

Group 3 - The HIA

Group 4 – Alberta Netcare EHR



Group 1—	-GPLM General
GPLM- FAQ-01- 0003- v1.0	Will the person's unmasked EHR be always viewable by the person's primary health care provider?
V1.0	No. GPLM applies to an individual's health information regardless of which authorized Netcare user needs to know that information. Even a family doctor or primary health care provider must unmask the record before viewing any of the patient's health information based on a need to know that information and <u>only</u> for that discrete episode.
	The patient record remains unlocked for the duration of the user's session and the mask resets after the user has logged out of Alberta Netcare Portal.
	The unmasking event is logged and subject to auditing.
GPLM- FAQ-01- 0004-	My patient has given me permission to unmask his EHR any time I need to. Is there a permanent unmask function that I can use?
v1.0	No. Alberta Netcare EHR clinicians that receive their patient's consent to unmask their record must still go through the unmask process <i>every time</i> they access the patient's record. This consent must meet the requirements established in the Health Information Act including but not limited to a date from which the consent is effective and a date that the consent will expire.
GPLM- FAQ-01- 0005-	Is a masked record in the Alberta Netcare EHR also masked in a physician's EMR?
v1.0	No. Global Person-Level Masking in Alberta Netcare does NOT mask an individual's health information in other electronic clinical information systems used by health care providers in Alberta.

GPLM-FAQ-02-0001v1.0

Who has the authority to mask an individual's health information?

Only custodians, such as Alberta Health Services, physicians and pharmacists who are participating in the Alberta Netcare EHR can respond to an individual's request for masking of their health information.

Custodians can delegate affiliates who can authorize a masking request within their organizations. Affiliates must exercise due diligence and comply with their professional practice standards. The following documents speak to the GPLM process:

- "Alberta Netcare Electronic Health Record Information Exchange Protocol", v2.1 (available from the HIA Help Desk at 780-427-8089 or hiahelpdesk@gov.ab.ca)
- "Guideline for Application for Global Person-Level Masking" (available from the Alberta Netcare Portal Login page https://portal.albertanetcare.ca/ab/NetcareLogin.htm).

Note: The custodian retains responsibility for decisions made by affiliates to authorize, refuse and rescind global person-level masking within the organization.

This authorization process requires that the custodian (or delegate) have the capacity to view the information in Alberta Netcare Portal to make the appropriate decisions related to masking.

GPLM-FAQ-02-0002v1.0

Can I delegate the authority to mask to another health care provider?

Yes - if you are a custodian with access to Alberta Netcare.

Custodians, such as Alberta Health Services, physicians, and pharmacists who participate in Alberta Netcare can respond to an individual's request for masking of their health information.

Custodians can delegate affiliates who can authorize a masking request within their organizations. Those affiliates must exercise due diligence and comply with their professional practice standards. The following documents speak to the GPLM process:

- "Alberta Netcare Electronic Health Record Information Exchange Protocol", v2.1 (available from the HIA Help Desk at 780-427-8089 or hiahelpdesk@gov.ab.ca)
- "Guideline for Application for Global Person-Level Masking" (available from the Alberta Netcare Portal Login page https://portal.albertanetcare.ca/ab/NetcareLogin.htm).

Note: The custodian retains responsibility for decisions made by affiliates to authorize, refuse and rescind global person-level masking within the organization.

This authorization process requires that the custodian (or delegate) have the capacity to view the information in Alberta Netcare Portal to make the appropriate decisions related to masking.

GPLM-FAQ-02-0003v1.0

What do I do if a patient in my care asks for their EHR to be masked?

If you meet the requirements to authorize Global Person-Level Masking for your patient, follow the *Guideline for Application for Global Person-Level Masking* document and take the opportunity to discuss the benefits and drawbacks of masking with the patient. This includes discussing:

- what a mask is,
- the situations that warrant unmasking, and
- any other risks that may be associated with applying a mask.

Include a description of how their health information will be accessed for treatment and care purposes.

In the event that you do not meet the requirements to authorize GPLM, direct the requesting individual to a custodian participating in the Alberta Netcare EHR <u>with whom the patient has a current care relationship and who is able to authorize the masking</u>.

This custodian must exercise due diligence and comply with their professional practice standards. The following documents speak to the GPLM process:

- "Alberta Netcare Electronic Health Record Information Exchange Protocol", v2.1 (available from the HIA Help Desk at 780-427-8089 or hiahelpdesk@gov.ab.ca)
- "Guideline for Application for Global Person-Level Masking" (available from the Alberta Netcare Portal Login page https://portal.albertanetcare.ca/ab/NetcareLogin.htm).

Those custodians able to authorize masking may include physicians, pharmacists, or Alberta Health Services.

GPLM-FAQ-02-0004v1.0

Can AHW set a mask in response to a request from an individual?

No. Due to the clinical implications of applying a mask, the request must be made to a custodian or delegate participating in Alberta Netcare.

This includes discussing:

- what a mask is,
- the situations that warrant unmasking, and
- any other risks that may be associated with applying a mask.

Include a description of how their health information will be accessed for treatment and care purposes.

If an individual is experiencing difficulty with the masking process, the health Information Act (HIA) Help Desk may be contacted to provide assistance:

- 780-427-8089 (Toll free by dialing 310-0000 followed by the phone number)
- <u>hiahelpdesk@gov.ab.ca</u>

GPLM-FAQ-02-0005v1.0

If I have helped my patient complete the application, and discussed masking and related issues, can I let my patient submit the form him/herself?

No. The custodian must fax the form to Alberta Health Services (AHS) who is responsible for actually setting or rescinding the mask.

The custodian should retain a copy of the form for their own records, regardless of whether or not they have chosen to authorize or rescind a mask.

GPLM-FAQ-02-0006v1.0

As a custodian, what do I do when a person asks for their EHR to be masked?

There are several steps to follow when applying for a mask – all of which are described in "Guideline for Application for Global Person-Level Masking". This guideline is available from the Alberta Netcare Portal Login page.

Administration Forms Multi User Amendment Form User Registration Form 3.01 (Oct 2008) Access Administrator Application for Global Person-Level Masking - Form and Guideline Application to Rescind a Global Person-Level Mask - Form and Guideline

The steps are:

- 1 Obtain the form "Application for Global Person-Level Masking" and "Guideline for Application for Global Person-Level Masking". These two documents are available from the Alberta Netcare Portal Login page.
- 2 If necessary, delegate this process to an affiliate.
- **3** Meet with the individual to:
 - a Confirm the individual's identity.
 - **b** Verify the person's Alberta Netcare EHR is not already masked.
 - c Discuss the benefits and drawbacks of masking. This includes discussing:
 - what a mask is.
 - the situations that warrant unmasking, and
 - any other risks that may be associated with applying a mask. Include a description of how their health information will be accessed for treatment and care purposes.
 - **d** Consider the consequences of masking this individual's EHR.
 - **e** If the individual wants to proceed with the mask, help them to complete the "Application for Global Person-Level Masking" form.
- **4** Fax the form to AHS Patient Information Services at 780-735-0646.
- **5** Retain an original copy (either paper or electronic) in the person's file.

Group 2	2—Applying or Rescinding a Mask
GPLM- FAQ-	How long does it take to set the mask on a person's EHR?
02- 0007- v1.0	Once the "Application for Global Person-Level Masking" form is faxed, Global Person-Level Masking will usually be set within three (3) business days.
	Incomplete or illegible forms may necessitate AHS-Edmonton Patient Information Services contacting the requesting individual or the custodian. This may delay the setting of the mask.

Alberta

GPLM-FAQ-02-0008v1.0

Can I refuse to mask a person's EHR?

Yes. If there are reasons to refuse the masking, for example, in the event of a public safety issue. The custodian is responsible for explaining the reasons for the denial to the requesting individual.

The individual then completes the top portion of the "Application for Global Person-Level Masking" form.

Netcare with record	APPLICATION FOR GL	OBAL PERSON-LEVE	L MA	SKING		
Date of Request						
Patient / Individual	(Last Name)	(First Name)	- —	(Middle	Name)	
Personal Health Number		Date of Birth (day/month/year)	_	1	1	
Gender: ☐ Male ☐ Female	Contact Phone Numbers		/			
REQUEST GLOBAL PERSON-L	EVEL MASKING					

I request that my health information on Alberta Netcare Electronic Health Record (known as Alberta Netcare) be masked so that it is not readily accessible to authorized users of Alberta Netcare. I understand that the requested mask only applies to my health information in the Alberta Netcare system. I understand that the masking may create some delay in my care. I further understand that my health information may be unmasked with or without my consent when deemed necessary. Reasons for unmasking will be noted by the authorized health services provider, and each unmasking will be logged and subject to auditing.

Signature of Patient / Authorized Representative (as per Section 104 of Health Information Act)

The custodian completes the REFUSAL TO AUTHORIZE portion of the form and documents the reason on the back of the form.

REFUSAL TO AUTHORIZE

I am unable to authorize the masking of this individual and have documented my explanation on the reverse side of this form. I will retain this form in the patient's files (in paper or electronic format). DO NOT FAX REFUSALS.

Signature of Authorizing Custodian

Print Name

Custodian's Phone #

Custodian / Affiliate's Organization & Address (at time form completed)

The original form is then placed on the individual's file in paper or electronic format (depending on the Custodian's preference).

DO NOT FAX any REFUSED application forms.

Group 2	2—Applying or Rescinding a Mask
GPLM- FAQ-	Where do I go for "masking" help?
02- 0009- v1.0	For further information related to the masking process or for assistance filling out the form, call the Health Information Act (HIA) Help Desk at 780-427-8089 or email: hiahelpdesk@gov.ab.ca
	For information about faxing to the AHS-Edmonton Patient Information Services and the technical application of the mask, call AHS Patient Information Services office at 780-735-0650.
GPLM- FAQ- 02-	What do I do if a patient in my care asks for their masked EHR information to be rescinded?
0010- v1.0	Direct the requesting individual to a custodian participating in the Alberta Netcare EHR with whom the patient has a current care relationship and who is able to rescind the mask.
	This custodian must exercise due diligence and comply with their professional practice standards. The following documents speak to the GPLM process: • "Alberta Netcare Electronic Health Record Information Exchange Protocol", v2.1 (available from the HIA Help Desk at 780-427-8089 or hiahelpdesk@gov.ab.ca) • "Guideline for Authorization to Rescind Global Person-Level Masking" (available from the Alberta Netcare Portal Login page https://portal.albertanetcare.ca/ab/NetcareLogin.htm).
	Those able to authorize rescinding the mask may include physicians, pharmacists, or Alberta Health Services.
	Note: The custodian who is asked to authorize the rescinding of the mask does not need to be the same custodian who originally authorized the application of the mask.
GPLM- FAQ- 02-	As a custodian, what do I do when a person asks for their masked EHR to be rescinded?
0011- v1.0	There are several steps to follow when rescinding a mask – all of which are described in "Guideline for Authorization to Rescind Global Person-Level Masking". This guideline is available from the Alberta Netcare Portal Login page.
	Administration Forms
	Multi User Amendment Form
	User Registration Form 3.01 (Oct 2008)
	Access Administrator Application for Global Person-Level
	Masking Form and Guideline Application to Rescind a Global
	Person-Level Mask - Form and Goldeline
	The steps are:
	1 Obtain the form "Authorization to Rescind Global Person-Level Masking" and

"Guideline for Authorization to Rescind Global Person-Level Masking". These two documents are available from the Alberta Netcare Portal Login page.

- 2 If necessary, delegate this process to an affiliate.
- **3** Meet with the individual to:
 - a Confirm the individual's identity.
 - **b** Verify the person's Alberta Netcare EHR is already masked.
 - **c** Discuss the implications of rescinding the mask in the Alberta Netcare EHR.
 - **d** If the individual wants to proceed with rescinding the mask, help them to complete the left side (A) of the "Authorization to Rescind Global Person-Level Masking" form.

A. REQUEST TO RESCIND GLOBAL PERSON-LEVEL MASKING BY INDIVIDUAL

I request that the Global Person-Level Mask applied to my health information be rescinded so that my health information is readily accessible by authorized users of Alberta Netcare. I understand that this request to rescind Global Person-Level Masking only applies to health information available through Alberta Netcare.

Signature of Patient / Individual / Authorized Representative (as per Section 104 of *Health Information Act*)

Signature of Authorizing Custodian

Print Name

Custodian's Phone #

Custodian/Affiliate's Organization & Address (at time form completed)

- **4** Fax the form to AHS Patient Information Services at 780-735-0646.
- 5 Retain an original copy (either paper or electronic) in the person's file.

Group 2	2—Applying or Rescinding a Mask
GPLM- FAQ-	Can I decide to rescind an individual's mask without their consent?
02- 0012-	Yes – if certain conditions are met.
v1.0	Custodians, such as Alberta Health Services, physicians, and pharmacists who participate in Alberta Netcare EHR can rescind (or delegate an affiliate to rescind) a masked EHR if:
	 The mask has consequences for public health and safety The masking process is no longer consistent with the custodian's professional practical guidelines There are other compelling reasons to rescind the mask.
	The custodian who rescinds the mask does not need to be the same custodian who originally authorized the application of the mask.
	This custodian must exercise due diligence and comply with their professional practice standards. The following documents speak to the GPLM process: • "Alberta Netcare Electronic Health Record Information Exchange Protocol", v2.1 (available from the HIA Help Desk at 780-427-8089 or hiahelpdesk@gov.ab.ca) • "Guideline for Authorization to Rescind Global Person-Level Masking" (available from the Alberta Netcare Portal Login page https://portal.albertanetcare.ca/ab/NetcareLogin.htm).
	The custodian retains responsibility for decisions made by affiliates to rescind global person-level masking within the organization.
	The individual's consent is not required to rescind a mask for the purposes outlined above; however they must be informed of the rescinding as soon as possible.
GPLM- FAQ-	What do I do if I can't meet the mask/rescind mask requestor face-to-face to discuss the consequences of their request?
02- 0013- v1.0	If it is not possible to meet in person, you may complete the form for the individual, if the person's identity can be verified.
	On the form, note that the individual's request was communicated by telephone.

GPLM-FAQ-02-0014v1.0

As a custodian, what do I do when I want to rescind a person's masked EHR?

There are several steps to follow when rescinding a mask – all of which are described in "Guideline for Authorization to Rescind Global Person-Level Masking". This guideline is available from the Alberta Netcare Portal Login page.

The steps are:

- **1** Obtain the form "Authorization to Rescind Global Person-Level Masking" and "Guideline for Authorization to Rescind Global Person-Level Masking". These two documents are available from the Alberta Netcare Portal Login page.
- **2** If necessary, delegate this process to an affiliate.
- **3** Identify the reason(s) why this mask should be rescinded.
 - The mask has consequences for public health and safety
 - The masking process is no longer consistent with the custodian's professional practical guidelines
 - There are other compelling reasons to rescind the mask.
- **4** Complete the right side (B) of the "Guideline for Application for Global Person-level Masking" form. Check the box that reflects the reason for the rescinding of the mask.

B. REQUEST TO RESCIND GLOBAL PERSON-LEVEL MASKING BY CUSTODIAN
As Custodian, I have determined that the Global Person-
Level Mask must be rescinded from the above
individual's health information accessible through Alberta
Netcare.
☐ For public health and safety reasons
☐ For other compelling reasons
□ Due to my professional practice guidelines
Signature of Authorizing Custodian
Print Name
Custodian's Phone #
Custodian/Affiliate's Organization & Address (at time form completed)
☐ The individual was informed on
that the mask will be
rescinded from his/her health information in
Alberta Netcare.
☐ The individual was not informed. Rationale for
proceeding with rescinding:

- 5 Inform the individual of the rescinding of the mask. Make a note of the date. If you are unable to contact the person after a number of attempts:
 - Record that the individual has not been informed.
 - Provide the rationale for rescinding the mask without contacting the individual on the form.
- **6** Fax the form to AHS Patient Information Services at 780-735-0646.
- **7** Retain an original copy (either paper or electronic) in the person's file.

Group 2	Group 2—Applying or Rescinding a Mask			
GPLM- FAQ-	How long does it take to rescind the mask on a person's EHR?			
02- 0015- v1.0	Once the "Guideline for Authorization to Rescind Global Person-level Masking" form is faxed, Global Person-Level Masking will be rescinded on Alberta Netcare usually within three (3) business days.			
	Incomplete or illegible forms may necessitate AHS-Edmonton Patient Information Services contacting the requesting custodian and may delay the rescinding of the mask.			
GPLM- FAQ- 02-	What are best practices for masking/rescinding masking of a person's Alberta Netcare EHR?			
0016- v1.0	1 Use the appropriate forms:			
V1.0	 "Application for Global Person-Level Masking" form, Sept 1 2008, v1.0 "Authorization to Rescind Global Person-Level Masking" form, Sept 1 2008, v1.0 			
	2 The custodian and individual should meet either face-to-face or by phone to discuss the risks and benefits of:			
	 masking the individual's EHR 			
	 rescinding the individual's masked EHR. 			
	3 If an individual's masked EHR is rescinded without their consent, the custodian should ensure that the individual is informed, and the rescind date and reason is marked on the form.			
GPLM- FAQ- 02-02-	As a custodian, what should I include in my discussion with the individual requesting the mask?			
0017- v1.0	Participating custodians who have a current care relationship with the requesting individual are required to discuss with him/her:			
	The risks and benefits of applying GPLM			
	 How his/her health information will be accessed for treatment and care purposes 			
	That unmasking may occur without consent in specific situations.			
	Custodians should also consider ethical and professionally-regulated issues related to applying the mask.			
	Content to include in your discussion is included in the form "Application for Global Person-Level Masking" form, Sept 1 2008, v1.0.			
GPLM- FAQ-	Do I have to keep a copy of the application to apply or rescind once it is sent?			
02- 0018- v1.0	Yes. Custodians should retain a copy of each applicable form.			

Group 2	Group 2—Applying or Rescinding a Mask		
GPLM-	Do I provide my patient with a copy of the signed form?		
FAQ- 02-	No. There is no reason for a nationt to ratein a convert the form. Forms are not		
02-	No. There is no reason for a patient to retain a copy of the form. Forms are not available to the general public.		
v1.0	available to the general public.		

Group 3	Group 3-HIA		
GPLM- FAQ- 03-	What is the HIA?		
0001- v1.0	The provincial Health Information Act (HIA) establishes the rules that must be followed for the collection, use, disclosure and protection of health information.		
	It balances the protection of privacy with enabling health information to be shared where appropriate.		
	The HIA sets out the rules that help to protect individuals' privacy through GPLM.		
GPLM- FAQ-	Who is a custodian?		
03- 0002-	According to the HIA, a custodian includes:		
v1.0	 Hospital boards, nursing home operators, provincial health boards, Alberta Cancer Board, etc. 		
	 Health care providers paid under the Alberta Health Care Insurance Plan to provide health services 		
	Licensed pharmacy and/or pharmacist.		
GPLM-	Who is an affiliate?		
FAQ- 03-	According to the HIA, an affiliate includes:		
0003-	 Employees of a custodian Any person that performs a service for a custodian (agent, appointee, 		
v1.0	volunteer or student)		
	 Health care providers who can admit/treat patients at hospitals and other health care practitioners with formal access to hospital resources. 		

Group 4 - ANP EHR GPLM-What is the Alberta Netcare Electronic Health Record (EHR)? FAQ-04-The Alberta Netcare EHR is a secure integrated record of an Albertan's key health 0001information. It is designed to give authorized health care providers across the v1.0 province access to a patient's health information such as: lab test results diagnostic imaging reports medications allergy and intolerance information personal demographic information. The Alberta Netcare EHR is a highly secure system that can only be accessed by authorized health care providers for treatment and care purposes. Those who access the Alberta Netcare EHR are trained in security measures and respect the privacy of health information. GPLM-Who is an authorized health care provider? FAQ-04-An individual who works at an authorized health care facility and has been granted 0002access to Alberta Netcare for direct patient care. The facility must have completed v1.0 privacy and security assessments prior to being accepted as an authorized facility. GPLM-Can any health care provider access an individual's EHR? FAQ-04-For security purposes, special authorization is required for health care providers to 0003access the Alberta Netcare EHR. User access is restricted based on their role and v1.0 profession. Authorized health care providers are asked for their unique usernames and passwords every time they access Alberta Netcare. The security controls utilized for the Alberta Netcare EHR are based on legislative requirements, security industry best-practices and standards of practice. Any access to the Alberta Netcare EHR is logged to an access log. These logs are audited monthly. Anyone who knowingly collects, uses, or discloses health information inappropriately could be subject to criminal charges, fines and disciplinary measures within their licensing or professional organizations.

Group 4 – ANP EHR

GPLM-FAQ-04-0004v1.0

How do I know if a patient's EHR is masked?

In Alberta Netcare Portal, the patient EHR will have a "lock" icon next to the individual's name. This indicates that their EHR is masked.

Search Results			
PHN / ULI	Name	Date of Birth	Age
<u>_</u> 87608-9200	MCDONALD, Mary	13-Apr-1964	45 y

It is not necessary to actually view an individual's lab and other data in order to determine if a mask has been set.



APPLICATION FOR GLOBAL PERSON-LEVEL MASKING

Date of Request						
Patient / Individual	(Last Name)	(First Name)	(Middle Name)			
Personal Health Number		Date of Birth (day/month/year)	1 1			
Gender: □ Male □ Female	Contact Phone Numbers	/				
REQUEST GLOBAL PERSO	N-LEVEL MASKING					
masked so that it is not mask only applies to my some delay in my care. consent when deemed r	I request that my health information on Alberta Netcare Electronic Health Record (known as Alberta Netcare) be masked so that it is not readily accessible to authorized users of Alberta Netcare. I understand that the requested mask only applies to my health information in the Alberta Netcare system. I understand that the masking may create some delay in my care. I further understand that my health information may be unmasked with or without my consent when deemed necessary. Reasons for unmasking will be noted by the authorized health services provider, and each unmasking will be logged and subject to auditing.					
Signature of Patient / Authori	zed Representative (as per Section 104 of Healt	h Information Act)				
APPLY GLOBAL PERSON-I	LEVEL MASKING					
information accessible the information. I find the	As Custodian, I have reviewed the relevant discussion points with the patient related to masking his/her health information accessible through Alberta Netcare. I am aware of no reason or requirement that would prohibit masking the information. I find the requested masking to be in accordance with my professional practice guidelines. I deem it appropriate that the masking be applied as requested.					
Signature of Authorizing Custo	odian	Print Name				
Custodian's Phone #	Custodian / Af	filiate's Organization & Address (at time f	form completed)			
REFUSAL TO AUTHORIZE						
I am unable to authorize the masking of this individual and have documented my explanation on the reverse side of this form. I will retain this form in the patient's files (in paper or electronic format). DO NOT FAX REFUSALS.						
ignature of Authorizing Custodian Print Name						
Custodian's Phone #	Custodian / Af	filiate's Organization & Address (at time f	form completed)			
FAX APPLICATION REQ	UESTS TO: CAPITAL HEALTH PATIEN	T INFORMATION SERVICES 780-7	735-0646			
	The mask will be set usually w	rithin 3 (three) business days.				
Questions? Contact the	Questions? Contact the HIA help desk at 780-427-8089 / Toll free Riteline at 310-0000 / hiahelpdesk@gov.ab.ca					
For Office Use Only						

Date Received:

Completed by:

Date Set:





THE AUTHORITY TO MASK

Only custodians who are participating in Alberta Netcare can respond to individuals' requests for masking of their health information. The authorization process outlined in the following document requires that the custodian (or delegate) have the capacity to view the information in Alberta Netcare to make the appropriate decisions related to masking.

DELEGATING THE AUTHORITY TO MASK

Custodians, such as Health Regions, physicians, and pharmacists, can delegate affiliates who can authorize a masking request within their organizations. Those affiliates must exercise professional judgment and comply with their professional practice standards as outlined in *IEP* v2.1 and the following guidelines. However, the Custodian retains responsibility for decisions made by affiliates to authorize, refuse and rescind global person-level masking within the organization.

SCRIPT FOR DISCUSSING ALBERTA NETCARE & GLOBAL PERSON-LEVEL MASKING

Alberta Netcare

Alberta Netcare is a secure lifetime record of an Albertan's key health information. It is designed to give authorized health services providers across the province access to a patient's health information such as lab test results, diagnostic imaging reports, medications, allergy information and personal demographic information. Alberta Netcare is a highly secure system that can only be accessed by authorized health services providers who use it to support patient care. Those who access Alberta Netcare are trained in security measures and respect the privacy of health information.

For security purposes, special authorization is required for health service providers to access Alberta Netcare and user access is restricted based on their role and profession. Authorized health services providers are asked for their unique usernames and passwords every time they access Alberta Netcare. The security controls utilized for Alberta Netcare are based on legislative requirements, security industry best-practices and standards of practice. Any access to Alberta Netcare is logged to an access log. These logs are audited monthly. Anyone who knowingly collects, uses, or discloses health information inappropriately could be subject to criminal

charges, fines and disciplinary measures within their licensing or professional organizations.

Global Person-Level Masking

For reasons of privacy, Albertans have the option of requesting that their health information in Alberta Netcare be "masked". All information about the individual can be masked except for first and last name, date of birth, gender and personal health number. This is called "Global Person-Level Masking". If approved, the mask is applied to an individual's health information within Alberta Netcare. Global Person-Level Masking makes accessing patient health information a two-step process. The health services provider must select the category (in a drop-down menu) that legitimately reflects the reason for the unmasking before the health information can be viewed. The six categories are:

- Patient Consent
- Direct Patient Care Clinical Need
- Medical Emergency
- Public Health Follow-up
- For Authorized Release of Patient Information
- As Required by Law

For example, every time a family doctor needs to read a patient's lab result or report, he/she will be required to unmask the patient's health information. Individuals whose health information is masked may experience minor delays in receiving treatment and care as their health information is unmasked.

Unmasking only applies to the health services provider's viewing of the health information for each discrete episode. When the health services provider logs out, or the system is shut down, the mask is reset. The unmasking of the masked health information is logged and subject to auditing (as are all viewings through Alberta Netcare).

Note: Global Person-Level Masking in Alberta Netcare does not mask an individual's health information in other electronic clinical information systems used by health services providers in Alberta.

(Rescinding the mask is done via the completion of the AUTHORIZATION to RESCIND GLOBAL PERSON-LEVEL MASKING form by the individual or Custodian.)

Sept. 1, 2008 v1.0 Page 2 of 4



	STEPS	CUSTODIAN RESPONSIBILITIES
1.	Print off or get copies of the APPLICATION for GLOBAL PERSON-LEVEL MASKING form.	The form: APPLICATION for GLOBAL PERSON-LEVEL MASKING can be printed from the Alberta Netcare Login page. It must be filled out, signed and submitted via secure FAX.
2.	Individual in your care asks that his/her health information in Netcare be masked.	The requesting individual is directed to a Custodian participating in Alberta Netcare with whom he/she has a current care relationship and who is able to authorize the masking (A participating custodian as defined by the <i>Information Exchange Protocol</i> v2.1). [May include physicians, pharmacists, nurses, etc. as determined by the Custodian organization.]
3.	Meet privately, face-to-face. If individual resides far away, complete process by phone. Fill out form on individual's behalf. Note on form if done by phone.	The recommended best practice is to undertake the following inquiries and discussion in a private, face-to-face meeting. However, if the individual and Participating Custodian are geographically distant, the Custodian can engage in the following discussion by phone provided that the identity of the individual can be verified. The Custodian completes the form for the individual and documents on the form that the request was transacted by telephone.
4.	Confirm individual's identity, and status as Authorized Representative, if applicable.	The Custodian ensures that the requested masking would apply to the health information: a: of the individual making the request, or b: of an individual for whom the requesting person is able to act as an authorized representative (as per Section 104 of the Health Information Act).
5.	View record to see if a mask is present. If not, proceed with next step. If mask in place, tell individual.	The Custodian logs onto Alberta Netcare to view the individual's record, or that of the individual represented, and checks for an existing mask. If not present, proceed with the process. If a mask is present, inform the individual.
6.	Discuss benefits and risks of masking with individual (see Script above.)	The Custodian engages the requesting individual, or authorized representative, in a discussion of the practical benefits and the potential risks of masking health information. This discussion would likely include some information on Alberta Netcare and its security features, and the occasions when subsequent unmasking may occur without the individual's consent (refer to the Script above).
7.	Consider individual's wishes and other considerations.	The individual's wishes are an important factor in deciding to proceed with the application of a mask. If, after a discussion of risks and benefits, the individual wants to continue the request, the Custodian must also consider: a: any consequences of masking to public health and safety b: any other compelling reasons to deny the request to mask c: any relevant professional practice guidelines to which the Custodian may be bound.

Sept. 1, 2008 v1.0 Page 3 of 4



STEPS	CUSTODIAN RESPONSIBILITIES
8. Have individual complete applicable portions of the form and sign. Fill out 'Custodian' portions of the form and sign.	If there is nothing to prevent the masking, the Custodian and requesting individual may fill out the APPLICATION for GLOBAL PERSON-LEVEL MASKING form (found on Alberta Netcare Login page).
REFUSAL: Explain the reason for refusing the masking to the individual and also note it on the back of the form. Place form in individual's file (in paper or electronic format). DO NOT FAX REFUSALS.	REFUSAL: If there are reasons to refuse the masking, the Custodian is responsible for explaining the reasons for the denial to the requesting individual. The individual completes the top portion of the form and the Custodian completes the REFUSAL TO AUTHORIZE portion of the form and documents the reason on the back of the form. The original form is then placed on the individual's file in paper or electronic format (depending on the Custodian's preference). DO NOT FAX any REFUSED application forms.
9. Fax form to 780-735-0646.	Fax the APPLICATION for MASKING form to Capital Health Regional Patient Information Services at 780-735-0646. (Note: Capital Health's RPIS office applies the technical Global Person-Level Masking function on behalf of Alberta Health and Wellness.)
10. Mask set usually within three business days.	Once faxed, the Global Person-Level Masking will be set on Alberta Netcare usually within three (3) business days. Incomplete or illegible forms may necessitate RPIS contacting the requesting individual or the Custodian and may delay the setting of the mask.
11. Retain original copy on individual's file (paper or scanned).	The original form is retained by the Custodian and can be kept on the individual's file in paper or electronic format.
Pressure.	The faxed copy will be kept on file in a locked cabinet at the Capital Health Regional Patient Information Services office. No follow-up notice will be sent to the requesting individual or the Custodian from Capital Health Regional Patient Information Services once the mask has been applied.

REFERENCE:

Alberta Netcare Information Exchange Protocol v2.1 Section 5.1: Masking of Information

ALSO SEE:

AUTHORIZATION TO RESCIND GLOBAL PERSON-LEVEL MASKING – Form and Guideline

NEED MORE HELP?

- ♦ For further information related to the masking process or for assistance filling out the form, call the HIA Help Desk at 780-427-8089 or email: hiahelpdesk@gov.ab.ca
- ♦ For information about faxing to the RPIS and the technical application of the mask, call Capital Health's Regional Patient Information Services office at 780-735-0650.

* * *

Sept. 1, 2008 v1.0 Page 4 of 4



AUTHORIZATION TO RESCIND GLOBAL PERSON-LEVEL MASKING

Date of Request					
Patient / Individual	(Last Name)		(First Name)	(Middle Name)	
Personal Health Number		Da	ate of Birth (day/month/year)	/	
Gender: ☐ Male ☐ Female	Contact Phone Numbers				
A. REQUEST TO RESCIND GLOBAL PERSON-LEVEL MASKING BY INDIVIDUAL I request that the Global Person-Level Mask applied to my health information be rescinded so that my health information is readily accessible by authorized users of Alberta Netcare. I understand that this request to rescind Global Person-Level Masking only applies to health information available through Alberta Netcare.			B. REQUEST TO RESCIND GLOBAL PERSON-LEVEL MASKING BY CUSTODIAN As Custodian, I have determined that the Global Person-Level Mask must be rescinded from the above individual's health information accessible through Alberta Netcare. □ For public health and safety reasons □ For other compelling reasons □ Due to my professional practice guidelines		
Signature of Patient / Individual / Authorized Representative (as per Section 104 of <i>Health Information Act</i>)			Signature of Authorizing Custodian		
Signature of Authorizing Custo	odian	Print Name			
Print Name		Custodian's	Phone #		
Custodian's Phone #		Custodian/A	Affiliate's Organization & Addres	ss (at time form completed)	
Custodian/Affiliate's Organiza	tion & Address (at time form completed)	res Alb	e individual was informed th cinded from his/her healt perta Netcare. e individual was not inform preeding with rescinding:	at the mask will be th information in	
EAV ADDITION DEC	HECTO TO: CADITAL HEALTH DATH	NIT INICOD	MATION CEDVICES 700 7	25 0646	

FAX APPLICATION REQUESTS TO: CAPITAL HEALTH PATIENT INFORMATION SERVICES 780-735-0646.

The mask will be set usually within 3 (three) business days.

Questions? Contact the HIA help desk at 780-427-8089 / Toll free Riteline at 310-0000 / hiahelpdesk@gov.ab.ca

For Office Use Only		
Date Received:	Date Set:	Completed by:



GUIDELINE FOR AUTHORIZATION TO RESCIND GLOBAL PERSON-LEVEL MASKING

(Can be requested by Individuals or initiated by Custodians)

A. HANDLING REQUESTS BY INDIVIDUALS TO RESCIND MASKING

STEPS		CUSTODIAN RESPONSIBILITIES
1.	Print off or get copies of the AUTHORIZATION to RESCIND GLOBAL PERSON-LEVEL MASKING form.	The form: AUTHORIZATION to RESCIND GLOBAL PERSON-LEVEL MASKING can be printed from the Alberta Netcare Login page. It must be filled out, signed and submitted via secure FAX.
2.	Individual in your care with masked health information asks that mask be rescinded. (Can be different Custodian than the one who authorized the masking.)	The individual is directed to a Custodian participating in Alberta Netcare with whom he/she has a current care relationship and is able to rescind the masking (A participating custodian as defined by the <i>Information Exchange Protocol</i> v2.1). [May include physicians, pharmacists, nurses, etc. as determined by the Custodian organization.] The Custodian who is asked to authorize the rescinding of the mask does not need to be the same Custodian who originally authorized the application of the mask.
3.	Meet privately, face-to-face. If individual resides far away, complete process by phone. Fill out form on individual's behalf and note on the form if done by phone.	The recommended best practice is for the Participating Custodian and individual to discuss the rescinding of the mask in a private, face-to-face meeting. However, if they are geographically distant, the Custodian can complete the form for the individual, providing his/her identity can be verified. The Custodian documents on the form that the individual's request for rescinding of the mask was transacted by telephone.
4.	Confirm individual's identity, and status as Authorized Representative, if applicable.	The Custodian ensures that the requested rescinding would apply to the masked health information: a: of the individual making the request, or b: of an individual for whom the requesting person is able to act as an authorized representative (as per Section 104 of the Health Information Act).
5.	View record to see if a mask is present. If mask in place, proceed with next step. If not, tell individual.	The Custodian logs onto Alberta Netcare to view the individual's record, or that of the individual represented, and checks for a mask. If present, proceed with the rescind process. If no mask is present, inform the individual.
6.	Fill out left side of the form (A) with individual and sign.	The Custodian and the individual, or the authorized representative, fill out the applicable portion (left side) of the AUTHORIZATION to RESCIND GLOBAL PERSON-LEVEL MASKING form (found on Alberta Netcare Login page).
7.	Fax form to 780-735-0646.	Fax the form to Capital Health Regional Patient Information Services office at 780-735-0646. (Note: Capital Health's RPIS office is responsible for the technical rescinding of all Global Person-Level Masks on behalf of Alberta Health and Wellness.)
8.	Mask is rescinded usually within three business days.	Once faxed, the rescinding of the Global Person-Level Masking will be completed on Alberta Netcare usually within three (3) business days. Incomplete or illegible forms may necessitate contacting the individual or the Custodian and may delay rescinding the mask.

Sept. 1, 2008 v1.0 Page 2 of 4



GUIDELINE FOR AUTHORIZATION TO RESCIND GLOBAL PERSON-LEVEL MASKING

(Can be requested by Individuals or initiated by Custodians)

STEPS	CUSTODIAN RESPONSIBILITIES
9. Retain hard copy on individual's file (paper or scanned).	The original form is retained by the Custodian and can be kept on the individual's file in paper or electronic format.
	The faxed copy will be kept on file in a locked cabinet at the Capital Health Regional Patient Information Services office. No follow-up notice will be sent to the individual or the Custodian from Capital Health Regional Patient Information Services once the masking has been rescinded.

B. CUSTODIAN-INITIATED AUTHORIZATION TO RESCIND MASKING

DELEGATING the AUTHORITY to RESCIND

Custodians, such as Health Regions, physicians, and pharmacists, can delegate affiliates who can initiate rescinding within their organizations. Those affiliates must exercise professional judgment and comply with their professional practice standards as outlined in *IEP* v2.1 and the following guideline. However, the Custodian retains responsibility for decisions made by affiliates to rescind global person-level masking within the organization.

	STEPS	CUSTODIAN RESPONSIBILITIES
1.	Print off or get copies of the AUTHORIZATION to RESCIND GLOBAL PERSON-LEVEL MASKING form.	The form: AUTHORIZATION to RESCIND GLOBAL PERSON-LEVEL MASKING can be printed from the Alberta Netcare Login page. It must be filled out, signed and submitted via secure FAX.
2.	When Custodians become aware of circumstances that no longer meet the conditions for masking, they may initiate the rescinding of a mask. (Can be different Custodian than one who authorized masking.)	The Participating Custodian identifies that one or more of the following has occurred for an individual whose information in Alberta Netcare is masked: a: The mask has consequences for public health and safety b: There are other compelling reasons to rescind the mask c: The masking is no longer consistent with the Custodian's relevant professional practice guidelines. The Custodian who rescinds the mask does not need to be the same Custodian who originally authorized the application of the mask.
3.	Fill out the right hand (B. Custodian) portion of the form, check one box, and sign.	The participating Custodian fills out the right side (B) of the AUTHORIZATION to RESCIND GLOBAL PERSON-LEVEL MASKING form (found on the Alberta Netcare Login page). The Custodian checks the box that best reflects the reason for rescinding the mask.
4.	Inform the individual by phone or in-person of the rescinding of the mask. Note on form the date when individual informed.	For the three circumstances noted in #2, the Custodian may rescind a mask WITHOUT the individual's consent. However, when a mask has been rescinded, the individual must be informed. It is the responsibility of the Custodian to inform the individual of the rescinding of the mask as soon as possible using secure means such as a telephone call or an in-person conversation. Please note on the form the date when the individual was informed that the mask is authorized to be rescinded.

Sept. 1, 2008 v1.0 Page 3 of 4



GUIDELINE FOR AUTHORIZATION TO RESCIND GLOBAL PERSON-LEVEL MASKING

(Can be requested by Individuals or initiated by Custodians)

	STEPS	CUSTODIAN RESPONSIBILITIES
5.	If unable to contact after reasonable attempts, note rationale on the RESCIND form.	If the Custodian has made reasonable attempts to contact the individual regarding the rescinding of the mask, he/she is to note that the individual has not been informed and document the rationale for proceeding with the rescinding in the absence of having contacted the individual.
6.	Fax form to 780-735-0646.	The Participating Custodian faxes the completed form to Capital Health Regional Patient Information Services at 780-735-0646. (Note: Capital Health's RPIS office is responsible for the technical rescinding of all Global Person-Level Masks on behalf of Alberta Health and Wellness.)
7.	Mask is rescinded usually within three business days.	Once faxed, the rescinding of the Global Person-Level Masking will be completed on Alberta Netcare usually within three (3) business days. Incomplete or illegible forms may necessitate contacting the Custodian and may delay rescinding the mask.
8.	Retain hard copy on individual's file (paper or scanned).	The original form is retained by the Custodian and can be kept on the individual's file in paper or electronic format.
		The faxed copy will be kept on file in a locked cabinet at Capital Health's Regional Patient Information Services office. No follow-up notice will be sent to the Custodian from Capital Health Regional Patient Information Services once the masking has been rescinded.

REFERENCE:

Alberta Netcare Information Exchange Protocol v2.1 Section 5.1: Masking of Information

ALSO SEE:

APPLICATION for GLOBAL PERSON-LEVEL MASKING - Form and Guideline

NEED MORE HELP?

- ♦ For further information related to the masking process or for assistance filling out the form, call the HIA help desk at 780-427-8089 or email: hiahelpdesk@gov.ab.ca
- ♦ For information about faxing to the RPIS and the technical application of the mask, call Capital Health's Regional Patient Information Services office at 780-735-0650.

* * *

Sept. 1, 2008 v1.0 Page 4 of 4

Government of Alberta

Provincial Logging and Audit Standard

September 2009

Health and Wellness

Alberta Health and Wellness Provincial Logging and Audit Standard Version 1.2

Developed and maintained by:

Information Compliance and Access Unit Information Management Branch Health System Performance and Information Management Division

1.0 Introduction

Health and Wellness

The Health Information Act (HIA) requires access to health information to be accessed on a need-to-know basis. Access logs play an important role in auditing user access, proactive monitoring and responding to breach investigations. In addition, system logs could facilitate the determination of system malfunctions and other system problems.

2.0 Purpose

- To identify data elements that require to be logged
- To identify logging requirements such as storage, log retention period and access to logged data.
- To develop provincial audit criteria.
- To put in place logging and auditing requirements that facilitate incident or breach investigation.

3.0 Scope

This standard applies to Alberta Health and Wellness (AHW), and all custodians under HIA including Alberta Health Services (AHS), physician and pharmacy offices, etc.

3.1 Systems under Consideration

- Any electronic system that collects, uses and discloses individually identifiable health information. Examples of such systems include Alberta Netcare and other clinical systems or applications.
- This standard applies to all systems or applications developed after adoption of the standard.
- Legacy systems or applications are out of scope of this standard but this standard should be retrofitted into existing legacy systems or applications, if feasible.

4.0 Standard

4.1 Logging

All accesses to systems or applications that collect, use and disclose individually identifiable health information such as Alberta Netcare applications and other clinical applications must be logged. Access to a patient's information must be logged and be subsequently displayed in the appropriate fields in the audit reports described below. Data elements will require to be logged each time an action is performed on patient information during an access. The following data elements must be logged when individually identifiable health information is accessed:

- User ID or application ID associated with an access: This is a unique identifier for a user or application. This data element should be logged once during an access to a patient's record.
- Name of user or application that performs an access. This is the full name of a user that accesses a patient's record. In the case of system-to-system communication, this is the application name. This data element should be logged once during an access to a patient's

record. For instance, if a user accesses a patient's record in the Pharmaceutical Information Network (PIN), the user's name should be logged once as long as the PIN session for that access stays alive no matter how long that session stays alive. This line of thought is used to describe logging requirements for subsequent data elements. If it is possible to derive the name of the user or application that performs the access from the user ID, then this data element should not be logged.

- Role (or profession or occupation) of a user who performs an access: This refers to the job function of a user performing an access. For instance, physician, pharmacist, nurse, etc. This data element should be logged once per access to a patient's record.
- Date of access: This refers to the day, month and year that a user or application performs an access. This should be logged once per access.
- Time of access: This refers to the hour, minute and second that an access is performed. This data element is logged each time an action is performed on a patient's record during an access. The time of access must be synchronised with local time.
- Actions performed by a user during an access: This may include one or a combination of the following: create, view, update or modify, delete, patient search, copy, print, etc. These data elements must be logged each time an action corresponding to any of the above is performed on a patient's record by a user during an access.
- Name of facility or organization of access: This data element should be logged once per access to a patient's record.
- Display Screen Number or Reference: This refers to the user interface or application that was used by a user during an access, for instance, PIN. This data element should be logged once per access.
- Stakeholder unique Identifier: This data element should be logged once per access to a patient's record. The unique identifier does not have to be part of the logs as long as it can be displayed in the audit report when needed. Example of unique identifier includes medical record number (MRN) and personal health number (PHN). One of these identifiers needs to be displayed in the audit report as two or more patients whose records have been accessed can have similar names.
- Stakeholder name: This is the name of the patient whose information is being accessed. This field should be logged once per access to a patient's record. If it is possible to derive the stakeholder name from the PHN without affecting the efficiency of the logging application, then, stakeholder name should not be logged.

As per section 41 of the HIA, the logs must provide complete information about a user who accessed a patient's information and about the patient whose information was accessed. The information that was accessed must be identifiable from the logs. In this respect, all data elements identified above must be logged.

4.2 Log storage, retention and access

Each custodian will determine an appropriate method for storing log data. Each custodian is responsible for ensuring that appropriate security controls are in place to protect logged data. Logs must be retained for an initial period of 10 years (see HIA section 41(2) or "Disclosure of Health Information" - HIA Guidelines and Practices Manual). Access to data in each log repository will be determined by the custodian. Since the logged data elements as defined above contain sensitive information such as individually identifiable health information, logs will be accessed only by affiliates with a need-to-know. Finally, log repositories and audit reports must not allow for the modification of logged data elements.

4.3 Audit

Access to systems or applications that collect, use and disclose individually identifiable health information will be proactively audited as deemed necessary by the custodian. In particular, as per the Privacy Impact Assessment for Alberta Netcare Portal, Alberta Netcare application access shall be audited on a monthly basis. In addition, a custodian or patient request or a breach could trigger an audit. A custodian or patient initiated audit will be performed as needed.

4.3.1 Application Audit Criteria

The following audit criteria have been identified:

4.3.1.1 Frequently Accessed Record Audit: This report generates information about patient records that have been accessed several times within a specified period of time. It also provides information about those who accessed the records.

Frequently Accessed Record Audit									
Report ID: Organization:									
Date:			Facility:	Facility:					
Time:									
Period From:			Period To:						
Trans. Date/	User ID	User Last	User First	Viewed	Patient	Patient	Number of		
Time		Name	Name	Patient Identifier	Last Name	First Name	Accesses		

4.3.1.2 User Name Search Audit: The report generates the list of users who accessed their personal records within a specified period of time. The main objective of this audit is to detect those who accessed their personal health information without going through the proper process. See Sections 7, 8, 10 and 11 of the HIA.

	User Name Search Audit								
Report ID:			Organizati	on:					
Date: Facility:									
Time:									
Period From:			Period To:						
Trans.	User	User	User	Viewed	Facility/	Patient	Patient		
Date/Time	ID	Last Name	First Name	Patient Identifier	Organization	Last Name	First Name		

4.3.1.3 Same User Same Patient Last Name Search Audit: This report generates a list of users who access the records of patients who have same last names as them within a specified period of time. It also provides information about the patients whose records were accessed by the user. The main objective of this audit is to determine users who accessed the health records of their family members without their consent.

	Same User Same Patient Last Name Search Audit								
Report ID: Organization: Date: Facility:									
Time:									
Period F	rom:			Period To	o:				
Trans.	User	User	User First	Application	Facility/Org	User Activity	Viewed	Patient	Patient
Date/	ID	Last	Name				Patient	Last	First
Time		Name					Identifier	Name	Name

4.3.1.4 Unmasking Decision Audit: This report provides information about a user who unmasked and accessed a patient's record within a specified period of time.

Unmasking Decision Audit							
Report ID:		Organiz	zation:				
Date:		Facility	:				
Time:							
Patient Identifier:	ent Identifier: Patient Name:						
Patient Age:		Patien	t Address:				
Period From:		Period	To:				
Unmasking date /time	User ID	User First Name	User Last Name	Application	Facility/ Organization	Unmasking reason	

4.3.2 Infrastructure Audit Criteria

The following audit criteria have been identified:

4.3.2.1 Lack of Use Audit: This report generates a list of users who have been inactive within a specified period of time.

	Lack of Use Audit							
Report ID:		Organization:						
Date: Facility:								
Time:								
Period From	:	Period To:	Period To:					
User ID	User	User First	Facility/	Last login	Inactive Days			
	Last Name	Name	Organization	Date/Time	After Last Login			

4.3.2.2 Frequent Failed Login Audit: This report generates the number of failed login attempts for each user within a specified period of time.

Frequent Failed Login Audit								
Report ID:		Organiz	ation:					
Date:		Facility:	Facility:					
Time:								
Period Fro	m:	Period	To:					
User ID	User Last Name	User First Name	Application	Facility/ Organization	Failed Login Date/Time			

4.3.3 Patient Activity Audit Reports

The following audit criteria have been identified:

4.3.3.1 Patient Activity Audit: This report provides detailed access for a particular patient within a specified period of time. This audit report will also facilitate breach investigation and/or patient access disclosure request.

		Pat	tient Activity Au	udit		
Report ID:	D: Organization:					
Date:		Facility:				
Time:						
Patient Identifier:	ifier: Patient Name:					
Patient Age:		Patient A	ddress:			
Period From:		Period To	o :			
Trans. Date/Time	User ID	User First	User Last	Application	Facility / Organization	
		Name	Name			

4.3.3.2 User Activity Audit: This report provides detailed access activities of a user within a specified period of time. This audit report will facilitate breach investigation for a user.

User Activity Audit								
Report ID:		Organiz	zation:					
Date:		Facility	:					
Time:								
User ID:		User N	lame:					
Period From:		Period	To:					
Trans. Date/Time	Application	Facility/Org	User	Viewed	Patient Last	Patient First Name		
			Activity	Patient Identifier	Name			

Linked Documents and Items

Name	Owner	Location

Definitions

Information: Combinations of data used to support specific business needs found in both databases and documents.

An Access: In this document, this refers to the operation of an authorized user reading or writing data or information to a storage device.

Versions

Version	Date	Revisions	Reviewers
1.0	November 2007	Initial standard	IPC Unit, Provincial Logging and Audit Standard Working Group
1.1	January 2008	Revised standard	AHW Architecture
1.2	September 2009	Revised Standard	ICA Unit
1.2	September 2009	Revised Standard	ICA Unit, Alberta Health Services
1.2	September 15, 2009	Approved Standard	IM/IT Strategic Planning Committee