Alberta
Netcare
ELECTRONIC HEALTH RECORD

ANP Quick Reference
Summary of Expedited Privacy Impact Assessment (PIA) Process

Purpose

The purpose of this document is to outline the expedited Privacy Impact Assessment (PIA) process for authorized custodians wanting access to Alberta Netcare via the provincial portal called Alberta Netcare Portal (ANP).

Support Contact Information

eHealth Services Team:

Phone: **1-855-643-8649** (toll free)
Email: ehealthsupport@cgi.com

The eHealth Services (eHS) team will assist health professionals to ensure that they meet the requirements for accessing Alberta Netcare and will provide training on the use of ANP.

PIA Requirements

Under the *Health Information Act* (*HIA*), custodians must submit a PIA to the Office of the Information and Privacy Commissioner (OIPC) of Alberta prior to implementing administrative practices and information systems relating to the collection, use or disclosure of individually identifying health information. A PIA must also be submitted before making any changes to those practices or systems.

The PIA is a due diligence tool for identifying and addressing privacy risks that may occur within a practice or information system. While PIAs are project specific, they do include an examination of organizational privacy practices. This includes implementing policies and procedures to support the *HIA* compliance.

The OIPC will review and comment on the PIA to ensure that the custodian has taken reasonable measures to protect privacy before providing acceptance of the PIA. The OIPC has developed a guide called Privacy Impact Assessment Requirements to assist in the completion of a PIA.

Included in the guide is the PIA template, in the form of a questionnaire that consists of five sections:

- Section A - Project Summary
- Section B - Organizational Privacy Management
- Section C - Project Privacy Analysis
- Section D - Project Privacy Risk Mitigation
- Section E - Policy & Procedures

Accessing Alberta Netcare

The requirements for becoming an authorized custodian are set out in the *Alberta Electronic Health Record (EHR) Regulation.* Requesting access to Alberta Netcare initiates the need for a new PIA. As part of the Alberta Netcare registration process, each custodian must complete an expedited ANP PIA and submit it to the OIPC.

Once the custodian provides confirmation to the eHSS team that their Alberta Netcare PIA has been submitted to the OIPC (following the expedited process below), Alberta Health initiates the next steps toward ANP deployment.

Expedited PIA Process

Since accepting the Alberta Health Netcare PIA in 2006 and again in 2013, the OIPC has agreed to allow authorized custodians to follow an expedited PIA process for accessing Alberta Netcare. Under the expedited PIA process, custodians must refer to the Alberta Health Netcare PIA and submit the following:

1 A formal OIPC cover letter that endorses the Alberta Netcare PIA (OIPC file #H3879) and includes an acknowledgement that the custodian:

- Has met all of the privacy and security requirements stated within the Alberta Netcare PIA.
- Understands their responsibilities and obligations when accessing Alberta Netcare.

- Understands that they are responsible for submitting a PIA amendment to the OIPC if there is a change to the *HIA* policies.
- Acknowledges that they are solely responsible for PIAs related to any other electronic health records systems that they control.

2 A copy of the custodian's policies and procedures that facilitate implementation of the *HIA* for their practice and that meet the following criteria:

- The custodian's professional college's Standards of Practice and the *HIA* requirements addressing health information management and protection must be reflected in the custodian's policies and procedures. (Health professional colleges and associations for custodians that may be authorized to use Alberta Netcare have prepared model policies that have been vetted by the OIPC. Please contact your professional college/association for more information.)
- The custodian must identify the specific organizational privacy management structure within their practice that addresses overall management of privacy functions. (This is included in the model policies provided by health professional colleges and associations.)

Summary of Key Information within the Alberta Netcare PIA

The following is a summary of key information contained within the Alberta Netcare PIA (H3879). It is being provided to the custodians to facilitate their ability to meet the expedited PIA requirement of endorsing the Alberta Netcare PIA. However, authorized custodians are responsible and accountable for ensuring that they meet all of the privacy and security requirements stated within the Alberta Netcare PIA. It is therefore important that custodians understand fully the commitments and responsibilities they undertake and accept when they make their submission. The custodians are thereby advised to review the entire Alberta Netcare PIA.

The Alberta Netcare PIA follows the OIPC PIA Requirements format. Information from each of the five sections, relevant to the custodian has been provided below.

Section A – Project Summary

Alberta Netcare is the name given to the Electronic Health Record (EHR). It is defined in the *HIA* as "the integrated provincial electronic health information system established to provide shared access by authorized custodians to prescribed health information in a secure environment." Alberta Netcare is accessible through the web-based provincial portal called ANP. ANP is designed to provide authorized custodians and their authorized affiliates access to prescribed health information within Alberta Netcare, pursuant to the *Alberta EHR Regulation* section 4. ANP is an entry point or viewer and does not contain any clinical information.

Alberta Health Services (AHS) operates and maintains ANP on behalf of Alberta Health. The *Alberta EHR Regulation*, section 2, designates Alberta Health as the information manager for Alberta EHR. An information manager is a person or body that performs one or more of the functions or provides one or more of the services as described in section 66(1) of the *HIA*. In this case, Alberta Health is providing information storage, retrieval, management and technology services to the custodians who are authorized to use Alberta Netcare.

Section B – Organizational Privacy Management

Alberta Health has established an EHR governance structure to ensure that access to identifiable health information is compliant with the *HIA*. The Information Exchange Protocol (IEP) provides the detailed rules and procedures for use, disclosure, right of access, integrity, and security of health information accessed by healthcare providers using Alberta Netcare, including roles and procedures for breach investigations. The rules contained within the IEP expand upon the obligations as documented in the *HIA*.

The IEP is part of the conditions understood and accepted by the custodian when they sign the Information Manager Agreement (IMA) with Alberta Health prior to gaining access or contributing to various components of Alberta Netcare. Signing the IMA commits the custodian and their affiliates to follow all of the rules. It is important for the custodian to read and fully understand these rules, because they will be responsible for making sure that everyone at their facility understands and follows them.

The custodian is responsible for ensuring that their affiliates 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 the *HIA* and regulations, as well as with their policies and procedures for their practice. In this regard, the custodian must provide training and awareness so that their affiliates understand the rules in the *HIA*, the implications of those rules, and administrative requirements. Alberta Health does provide training and awareness materials to custodians regarding access to Alberta Netcare.

The custodian is responsible to collect, use, disclose and protect health information within its custody and control in accordance with provisions set out in the *HIA*. The custodian has a duty to identify its affiliates (e.g. employees, Information Managers, and persons who provide services for the custodian) and to take steps to ensure they comply with the *HIA* and the custodian's policies and procedures. It must be understood that an affiliate's collection, use or disclosure of health information is considered to be a collection, use or disclosure by the custodian.

To ensure consistency and effectiveness of responses to health information under threat, Alberta Health has instituted the Provincial Reportable Incident Response Protocol (PRIRP) for all authorized custodians and their affiliates managing or accessing Alberta Netcare. This process covers breaches of data confidentiality, data integrity and data availability.

Users who do not follow Alberta Netcare security and privacy policies, protocols or procedures can have their access privileges revoked. If an Alberta Netcare user deliberately breaches health information or attempts to gain unauthorized access to health information in the system, they can be prosecuted under the HIA and fined. Their professional regulatory bodies or employer may also bring disciplinary action against them.

Section C – Project Privacy Analysis

Alberta Netcare components are described within the document, An Overview of Alberta's Electronic Health Record Information System (EHRIS). Information within Alberta Netcare is automatically captured from point of care data systems such as pharmacies, labs, diagnostic services and AHS systems. When updates are made to the information within those systems, those systems automatically update Alberta Netcare. A detailed data availability report is available to registered Alberta Netcare users from the ANP Login page.

The *HIA* governs the collection, use, disclosure and protection of health information in the custody or control of custodians. When authorized custodians and their affiliates access Alberta Netcare, it is considered a "use" of the health information.

It is important for the custodians to understand that Albertans have the option of requesting that their health information in Alberta Netcare be "masked." This means that the individual's health information will not be automatically visible. This enables custodians and their affiliates to actively consider an individual's expressed wish to limit the availability of their information through Alberta Netcare.

Section D - Project Privacy Risk Mitigation

Access to Alberta Netcare is role-based. Users are only permitted to access information that is relevant to their role in the health system. This means that access permissions and other security credentials will be set up so that users have information on a "need-to-know" basis.

The custodians from community sites must conduct a Provincial Organizational Readiness Assessment (pORA), as they are outside of the Alberta Health Services/Covenant Health secure zone. This tool assesses the custodians' administrative, technical and physical security controls in order to mitigate risks of accidental or malicious access to health information. It is an auditing tool and process to ensure that each authorized custodian has the required processes and measures in place to handle access in compliance with Alberta EHR governance.

Access via ANP is provided through secure networks (such as those in AHS facilities) or securely over the internet using two-factor authentication. Two-factor authentication involves a password and user ID to be used in conjunction with an authentication device (RSA SecurID token). Both must be present for the individual to gain access to Alberta Netcare if outside of the secure network.

A number of security safeguards are in place to make sure that only authorized users can access Alberta Netcare. These include multiple levels of access controls and encryption. The security controls used to protect information in Alberta Netcare are based on international standards and best practices. All electronic messages that are shared are encrypted, which means that the information is encoded. Additional network security controls include the use of firewalls and an intrusion detection system to alert the appropriate personnel of any unusual activity.

All ANP accesses are logged and a provincial-level audit function is in place to ensure that the information is accessed appropriately. Both complaint-based and proactive audits are conducted. An individual can request a report from Alberta Health to find out who has been accessing their health information, and when. Alberta Health will follow up with the authorized custodian if a breach is suspected. Alberta Health will also periodically request that the authorized custodian re-validate that their access is appropriate and required.

It is important that custodians are familiar with the privacy risks identified within the Alberta Netcare PIA, and understand their role in mitigating those risks. The following identifies three key risks and the security safeguards to be put in place to mitigate those risks when accessing Alberta Netcare:

Risk 1
There could be unauthorized or inappropriate browsing of patient data via ANP

Mitigation:

1. Access Controls:
   a. A permission matrix that defines user roles and restricts access based on the *HIA*.
   b. The PRIRP outlines the actions to be taken in the event of a security breach.
2. Training
   a. Users are supported through education and training regarding the use of ANP, underlying applications, and other privacy and security obligations.
   b. The PRIRP outlines the actions to be taken in event of a security breach.
3. Auditing
   a. All accesses are logged and a provincial level audit function process is in place.
   b. An individual can request a report from Alberta Health to find out who has been accessing their health information, and when.
   c. Users will be periodically requested to re-validate that their access is appropriate.
   d. Audit reports/findings will be followed up with the custodian/regulatory body.
4. Custodian Obligation
   a. Under the *HIA*, the custodian is responsible to maintain administrative, technical, and physical safeguards to protect the privacy and confidentiality of health information in their custody. Community authorized custodians must submit a pORA.
   b. The custodian has a duty to ensure their affiliates comply with the *HIA* and the custodian's policies and procedures.

Risk 2
There may be a loss of data integrity (accuracy and consistency), destruction or unauthorized use of health information.

Mitigation:

1. Encryption:
   a. All data transfers outside of the secure network will be encrypted. All ANP access will be via HTTPS.

b. Mobile devices must be encrypted.

2. Network Security Controls:

a. Implementation of intrusion prevention system, firewalls, and fully redundant infrastructure, with automated failover and recovery. These have regularly updated protection.

b. The PRIRP outlines the actions to be taken in event of a security breach.

c. Business continuity plans are in place in an event of a disaster (e.g. fire).

Risk 3

There is a risk that a subcontractor will not appropriately manage privacy and security of EHR data.

Mitigation:

Third party vendors must sign an agreement that include security, access and confidentiality clauses that obligate adherence to legislation, standards, policies and information management requirements of the custodian.

Section E – Policy & Procedures

The table details Alberta Health’s organizational policies that facilitate compliance with the HIA. The custodians must also implement policies and procedures that facilitate the HIA compliance within their practice. (Custodians append their own policies to their expedited Alberta Netcare PIA submission, as described above on page 1, under Expedited PIA Process.)