Privacy Officer Handbook

Published: February 2015

Alberta Netcare ELECTRONIC HEALTH RECORD

Table of Contents

The information in this handbook is provided for education and guidance only and is not intended to replace expert advice. Physicians are responsible for making informed decisions to meet their medical-legal obligations.

Important Contacts

Stakeholders and Authorities	For Assistance With
Alberta Netcare www.albertanetcare.ca 1.844.542.7876	Alberta Electronic Health Record (Alberta Netcare) eHealth Support Team: enrolment, use, support security and privacy
Health Information Act (HIA) Help Desk 780.427.8089	HIA compliance, questions specific to Alberta Netcare or Alberta Health as Information Manager of Netcare
Office of the Information and Privacy Commissioner of Alberta www.oipc.ab.ca 1.888.878.4044	PIA submission and review, HIA compliance and privacy incident investigations
College of Physicians & Surgeons of Alberta www.cpsa.ab.ca 1.800.561.3899	Privacy issues involving physicians, ownership of patient records or patient records retention

Introduction

The relationship physicians have with their patients is based on trust. Your patients trust you to make the right decisions for their health and they trust you and your staff to protect their health information.

Your patients expect their privacy to be protected when they seek medical care in Alberta health facilities. Alberta legislation grants that right to individuals, and it also outlines a number of requirements that apply to health care professionals. This includes designating a clinic privacy officer.

This handbook presents the various duties a privacy officer must assume in a clinic and provides useful information about how privacy officers can meet the expectations that come with this role.

Designating a Clinic Privacy Officer

Your clinic's privacy officer is the "go to" person for information about Alberta's Health Information Act (HIA). This individual is responsible for ongoing privacy and security policies and practices, and for emerging privacy and security issues that impact your clinic's operational processes.

The appointment of a designated privacy officer is a key aspect in a clinic's protection of privacy and health information. A privacy officer will oversee the clinic's privacy and security efforts and ensure compliance with the law. The clinic privacy officer role is a requirement under the HIA.

The privacy officer can be a clinic physician or a responsible affiliate (for example, a clinic manager). When designating a privacy officer for your clinic, consider the following important skills the person of your choice should have:

- An understanding of electronic medical record (EMR) technology
- Familiarity with privacy principles
- Knowledge of the clinic's operations
- Rapport with clinic physicians and staff

A privacy officer provides critical care for a clinic's patient health information

A designated privacy officer is a requirement whether your clinic uses paper records, electronic records or a mix of the two.

- It is vital that everyone in the clinic know who the privacy officer is in order to direct incoming requests and emerging issues appropriately.

- The privacy officer usually performs the duties of a security officer as well, since privacy and security are closely related especially in the context of HIA compliance. It is important to note the privacy officer often depends on the EMR or I.T. Support vendor for many security functions, especially those of a technical nature.

Responsibilities of a Clinic Privacy Officer

The following list outlines the duties for which the clinic privacy officer is responsible, along with practical implications for each of these.

Develop privacy policies and procedures and keep them up to date

- Develop or maintain privacy policies and procedures that are easily accessible, and easy to read and understand.
- Include all aspects relevant to your clinic's operations and to the handling of patient information.

Ensure clinic staff and vendors are aware of their privacy obligations

- Provide new hires with a privacy orientation session.
- Make new vendors aware of clinic privacy policies and procedures.
- Make these policies and procedures available to all staff and vendors.

Monitor your clinic's ongoing compliance with the HIA

- Make sure that routine handling of health information follows the principles outlined in your privacy policies and procedures.
- Enforce policies and procedures with staff and vendors as needed.
- Complete privacy and security self-assessments annually to ensure ongoing compliance with the HIA.
- Stay aware of changes that may affect your clinic and evaluate the need to update your clinic's privacy impact assessment (PIA).

Act as the primary point of contact for staff and third parties such as patients, vendors and authorities

- Receive and respond to requests for access to and correction of health information from patients.
- Answer questions from physicians and clinic staff.
- Be the liaison with the Office of the Information and Privacy
- Commissioner (OIPC) of Alberta.

Privacy Breach Management Procedure

A privacy breach can take place when there is unauthorized access to, collection of, use of, disclosure of or disposal of personal or health information.

A (suspected) privacy breach should be identified and immediately reported to the clinic privacy officer and clinic manager. The privacy officer completes the following steps with assistance of the affected physician(s):

- Immediately contain the breach by stopping the unauthorized access, recovering the records, shutting down the system that was breached, revoking access and correcting weaknesses in physical security.
- Contact the clinic's EMR vendor support and/or I.T Support personnel and ask if they can help address the breach situation.
- Notify the police if the breach involves theft or criminal activity.
- Ensure any breach involving Alberta Netcare is immediately reported to the Information Access and Privacy Office at 780.427.8089 or toll free at 310.0000.

Privacy officers may also contact the two following organizations for guidance or assistance. If you intend to seek advice from the OIPC regarding how to respond to the breach and what actions should be taken, you should report the incident as soon as possible.

OIPC

Edmonton 780.422.6860

1.888.878.4044

College of Physicians & Surgeons of Alberta

780.423.4764

1.800.561.3899 (in Alberta only)

Privacy Officer Tips

The biggest privacy risk is internal misuse. Here are some tips to reduce your risk as it relates to staff:

- Engage employees so they feel accountable and involved.
- Act and be seen as a partner in privacy and security compliance.
- Network and communicate frequently.
- Develop and offer tools to make compliance easy.
- Embed awareness of clinic privacy requirements in staff behavior and organizational culture. Privacy is not an afterthought.
- Implement role-based hands-on procedures.

Develop a process for updating privacy policy information

- This enables you to respond to new issues as they arise and provide ongoing updates to employees to ensure that they can respond appropriately in the circumstances.

Review patient/client complaints and identify common issues

- This strategy will help you address concerns about your privacy policies and practices, and enhance your privacy training program.

Let employees know where to go for help

- While it is not possible to anticipate every question that patients will ask, providing key information and access to resources or individuals within the organization who can provide further information will help both patients and employees understand the clinic's practices.

Conduct privacy and security self-assessments on an annual basis

- Privacy and security self-assessment templates allow you to review your clinic's policies and procedures, and can indicate where you need to improve clinic procedures.

Complete online privacy training programs

Visit http://www.albertanetcare.ca/LearningCentre/EMR-Privacy.htm and select the next Privacy Training document.

Clinic Privacy Officer Duties

Privacy Documentation	Initial	Annual	Ongoing
Ensure that clinic privacy and security policies and procedures are developed and maintained to remain current.			
Develop or customize privacy and security policies. Involve clinic physicians and staff to ensure understanding and compliance. Use established resources as a starting point for clinic policies. Your PIA binder includes the following resources: Health Information Privacy and Security Manual Clinic Policies and Procedures Risk Assessment	✓ ✓		
Maintain clinic policies so that they stay current with regulatory requirements.			✓

Privacy Documentation	Initial	Annual	Ongoing
Require vendors to advise you as privacy officer of any changes to their privacy and security policies and procedures during the length of the contract. Review changes provided to ensure adherence to your clinic's policies and procedures and HIA requirements.			✓
Maintain an electronic or paper copy of the clinic PIA(s) in your business records at all times.			✓
Implement and maintain archives and destruction logs. Review the records retention policies.	✓		✓
Create a privacy officer journal and update it chronologically.	✓		✓
Document changes with vendors, policies, practices, staffing, physical security, computer hardware and software. This journal is maintained for the duration of the clinic—it is not unique to the individual who fills this role.	✓		✓

Privacy Awareness of Staff and Other Agents	Initial	Annual	Ongoing
Ensure that the clinic's physicians and affiliates are aware of and have access to the clinic's privacy and security policies and procedures.			
Deliver or organize initial training for new affiliates (for example, staff, volunteers or students) on the HIA and the clinic's policies and procedures.	✓		
Build confidentiality expectations and consequences into employee job descriptions.	✓		✓
Use staff meetings, bulletins, communication logs, in-services and workshops to ensure clinic affiliates are aware of their responsibilities under the HIA.			✓
Deliver or organize annual training refreshers and ongoing training for clinic staff and contractors as best practices change or the HIA is updated.		✓	✓
Ensure clinic vendors and other agents are aware of their responsibilities and duties.			
Deliver or organize initial training for new vendors and contractors on the HIA and the clinic's policies and procedures.	✓		

Privacy Awareness of Staff and Other Agents	Initial	Annual	Ongoing
Give all vendors and other third parties a copy of the clinic's privacy and security policies and procedures, and have them sign a declaration to confirm receipt.	✓		
Require vendors to review the clinic's privacy and security policies and procedures annually.		✓	
Advise clinic vendors when clinic privacy and security policies have changed.			✓

Privacy Compliance Monitoring	Initial	Annual	Ongoing
Ensure the overall security and protection of health information in the custody or control of the clinic.			
Implement and maintain clinic administrative, technical and physical safeguards to protect patient health information.	✓		✓
Undertake regular privacy practice reviews to keep your practices current.		✓	✓
Ensure you have the authority, support and resources to do a proper job.	✓		✓
Complete or assist with writing the clinic's PIA.	✓		
Update the clinic's PIA annually to reflect any physical, technical or administrative changes that may affect the collection, use or disclosure of personal health information in the physician's care or control (for example, change in clinic location, undertaking a data migration project or a change in EMR vendor).		✓	✓
Ensure a disclosure log is implemented and used consistently.	✓		✓
Determine if an Information Sharing Agreement is necessary (usually required when there is more than one physician at a location).	✓		✓
Protect clinic staff personal information according to the *Personal Information Protection Act* (PIPA).			✓

Privacy Compliance Monitoring	Initial	Annual	Ongoing
Coordinate and facilitate clinic privacy compliance activities. Identify privacy compliance issues and provide training and guidance to clinic custodians and affiliates.			
Have employees sign a confidentiality agreement when they commence employment at the clinic and annually thereafter.	✓	✓	
Before hiring a third-party vendor, check into their security and privacy policies and practices to help ensure confidence that vendors will keep patient information confidential and secure.	✓		
Have vendors review and execute an Information Manager Agreement or Vendor Non-Disclosure Agreement. Follow-up to ensure they implement safeguards and review periodically.	✓		✓
Oversee the selection, testing, deployment and maintenance of security hardware and software products and any related third-party services.	✓		✓
Oversee IT processes including backup schedule, backup restore testing, EMR/ software installation, EMR access authorization and role-based access matrix.	✓	✓	✓
Ensure that appropriate resources required during a systems failure are identified and appropriate contractual arrangements with adequate service levels are in place.	✓		✓
Respond to real or suspected breaches of privacy by taking common sense steps to limit the breach. Follow steps outlined in the Privacy Breach Management Procedure on page 4. Notify appropriate third parties depending on the nature and extent of the incident.			✓
Review and act on all reports following a privacy incident. Follow steps in the clinic policies.			✓
Stay apprised of HIA developments such as legislation changes, OIPC orders, OIPC rulings on patient complaints, or new directions from the CPSA.			✓

Primary Point of Contact for Privacy-Related Inquiries	Initial	Annual	Ongoing
Act as the clinic primary contact in regard to the HIA and clinic privacy and security policies.			

Primary Point of Contact for Privacy-Related Inquiries	Initial	Annual	Ongoing
Be familiar with obligations under the HIA.	✓		✓
Make yourself known to the physicians and staff as the primary privacy resource for the clinic.	✓		✓
Provide clinic physicians and staff with advice regarding HIA compliance.			✓
Respond to requests for access to or correction of health information.			
Answer patient inquiries and questions regarding privacy and clinic practices.			✓
Ensure access and requests are documented consistently.			✓
Ensure expressed wishes of an individual are documented consistently.			✓
Call Alberta Health's HIA Helpdesk or the OIPC if you require clarification or guidance (see Important Contacts on page 2 for phone numbers).			✓
Act as the main point of contact in dealings with third parties, Alberta Netcare, OIPC, researchers, regulatory bodies or the police regarding privacy and security policies, procedures or incidents.			
Document each issue and outcome.			✓
Review research requests and decide if the clinic will disclose health information for research purposes. Enter into a Research Agreement with the researcher per the HIA before disclosure of any health information.			✓
Receive, investigate and respond to complaints and/or alleged violations with regards to the clinic's collection, use and disclosure of or access to health information.			
Use the HIA Guidelines and Practices Manual and other resources as needed to guide your investigation and response.			✓
Conduct investigations into processes and procedures affecting HIA compliance or clinic privacy and security policies and procedures.			✓
Document each privacy breach or suspected privacy breach, its investigation, recommendations and lessons learned.			✓

Privacy Officer Journal

The privacy officer journal is an administrative document of the clinic. When a new person becomes the clinic privacy officer, the journal should be passed to each subsequent incumbent. The privacy officer journal can be maintained electronically, in notebook format or as a binder—choose the format that is convenient and most likely to be maintained consistently over time.

Sample format:

Date	Type of Note	Notes
2014-Jan-31	Change in EMR access request policy	New clinic physician and staff required to fill out EMR access request form prior to account creation

Privacy Resources

- Health Information – A Personal Matter, A Practical Guide to the Health Information Act (amended August 26, 2010) - Office of the Information and Privacy Commissioner of Alberta
  - www.oipc.ab.ca/pages/Resources/HIA.aspx (under Guides)
- Health Information Act Guidelines and Practices Manual March 2011 Alberta Health
  - http://www.health.alberta.ca/documents/HIA-Guidelines-Practices-Manual.pdf
- Online Privacy Training
  - http://www.albertanetcare.ca/LearningCentre/EMR-Privacy.htm

Important Contacts

Stakeholders and Authorities	For Assistance With
Alberta Netcare www.albertanetcare.ca 1.855.643.8649	Alberta Electronic Health Record (Alberta Netcare) eHealth Support Team: enrolment, use, support security and privacy
Alberta Health HIA Help Desk 780.427.8089	HIA compliance, questions specific to Alberta Netcare or Alberta Health as Information Manager of Netcare
Office of the Information and Privacy Commissioner of Alberta www.oipc.ab.ca 1.888.878.4044	PIA submission and review, HIA compliance and privacy incident investigations
College of Physicians & Surgeons of Alberta www.cpsa.ab.ca 1.800.561.3899	Privacy issues involving physicians, ownership of patient records or patient records retention

Glossary

This section provides definitions of terms used in applicable privacy legislation and clinic policies and procedures.

Term	Definition
Affiliate	An individual employed by a custodian; a person who performs a service for the custodian as an appointee, volunteer or student under a contract or agency relationship with the custodian; and a health services provider who has the right to admit and treat patients at a hospital as defined in the *Hospitals Act*. Source: Health Information Act: Guidelines and Practices from Alberta Health
Authorized representative	Any person who can exercise the rights or powers conferred on an individual under applicable privacy legislation. This includes the right of access to an individual's health information and the power to provide consent for disclosure of such information.
Collection	To gather, acquire, receive or obtain health information. Source: *Health Information Act*, Section 1(1)(1)(d)

Consent	An individual giving permission to have his or her information collected, used or disclosed to someone else. When consent is given, it must be documented, given for a specific purpose and duration, freely obtained and informed.
Custodian	A health services provider, individual, board, panel, agency, corporation or other entity designated as a custodian in the *Health Information Act* (HIA) or regulations, responsible for compliance with the HIA. Custodians under the HIA include: • Physicians and Surgeons • Pharmacists • Optometrists • Opticians • Chiropractors • Midwives • Podiatrists • Denturists • Ambulance Operators • Registered Nurses • Dentists and Dental Hygenists • Hospital Boards • Provincial Health Boards • Alberta Health. Source: *Health Information Act*, Section 1(1)(f)
Disclosure	The act of revealing, showing, providing copies, selling, giving or relaying the content of health information by any means to any person or organization.
Expressed wish	Instructions given by a patient to a health services provider with regards to disclosures of their health information. This request must be documented and considered before subsequent disclosures of information.
Health information	One or both of the following: (i) diagnostic, treatment and care information; (ii) registration information or both; Source: *Health Information Act*, Section 1(1)(k)
Health Information Act (HIA)	An act of the Alberta legislature governing an individual's right to request access to health records in the custody or under the control of the custodians, while providing custodians with the framework within which they must conduct the collection, use and disclosure of health information. The act also covers the actions of affiliates.

Information manager	Person or body that stores or provides one or more of the following services and functions: • Processes, stores, retrieves or disposes of health information • Strips, encodes otherwise transforms, individually identifying health information to create non-identifying health information (in accordance with the regulations) • Provides information manager or information technology services Examples include EMR vendors, shredding companies, IT services companies, transcription service companies or anybody who encodes or modifies health information.
Information Manager Agreement (IMA)	A legislative requirement when a custodian hires an information manager which must contain clauses that address the following (note that this list is not exhaustive): • Services to be provided by information manager to the custodian • Information manager's authority to collect, use or disclose health information provided by the custodian • Responsibilities of information manager under this agreement • Indemnity and Hold Harmless – the information manager's accountability for all requirements identified in this agreement • Policies and procedures to protect health information • Term and termination of the agreement Source: *Health Information Act*, Section 66(2) and Health Information Regulation, Section 7.2

Information Sharing Agreement (ISA)	In the context of EMR implementations, the legal contract between clinic organizations and EMR vendors that defines the data stewardship rules and processes to which the parties have agreed. It establishes the roles, expectations and accountabilities of each of the parties in their stewardship of the medical information in their custody. The information sharing agreement (ISA) represents the operational application of health policy by physicians, and is a major determinant for the structure and processes in EMR deployments and other medical record initiatives. According to the College of Physicians & Surgeons of Alberta key elements of an ISA include: • Identification of the needs and objectives of the key stakeholders • Principles that guide the development and maintenance of the agreement • Details of the information uses and disclosures • Details of the products and services available • Transition services (entering and exiting the agreement) • Record retention and access • Definition of the service levels • Roles and responsibilities of each party to the agreement • Financial and legal terms • Governance and administration processes (including the makeup of the governing body and the dispute resolution process)
Office of the Information and Privacy Commissioner (OIPC)	An Alberta office established in 1995 to assist the Commissioner to fulfill a mandate under the *Freedom of Information and Protection of Privacy Act*. In 2001, the Commissioner's jurisdiction expanded to include regulatory responsibilities for the *Health Information Act*. In January 2004, the Commissioner was given oversight responsibilities for the *Personal Information Protection Act*.
Personal Information Protection Act (PIPA)	An act of the Alberta legislature that protects individual privacy by requiring, in most cases, private-sector organizations to obtain consent for the collection, use and disclosure of personal information and providing individuals with a right of access to their own personal information.

Privacy breach	In general terms, a violation of a privacy rule or law. In the context of privacy, any unauthorized access, collection, use, disclosure, loss or destruction of health information protected under the *Health Information Act*, or other information protected under other acts.
Privacy impact assessment (PIA)	A due diligence exercise in which a custodian responsible for collecting, using and disclosing health information identifies, analyzes and addresses potential privacy risks that may occur in the course of a clinic's operations. Privacy impact assessments assist custodians in reviewing the impact that new programs, systems and practices may have on individual patient privacy and ensure that changes are evaluated to be compliant with the *Health Information Act*.
Privacy officer	An individual who is a custodian or an affiliate and who is designated to be responsible for: • Developing policies and procedures and keeping them up to date. • Ensuring that individuals working at or for a clinic are aware of their obligations. • Monitoring ongoing compliance with the Health Information Act. • Acting as a primary point of contact for patients and other organizations like the Office of the Information and Privacy Commissioner or other regulatory bodies.
Record	Information in any form, including notes, images, audiovisual recordings, books, documents, maps, drawing, photographs, letters, vouchers, papers and any other information that is written, photographed, recorded or stored in any manner. Does not include software or any mechanism that produces records. Source: *Health Information Act,* Section 1(1)(t)
Use of health information	To apply health information for a purpose, including reproduction of the information. Accessing information available through Alberta Netcare is considered a use, not a collection. Source: *Health Information Act*, Section 56.5(2)
Vendor Non-Disclosure Agreement (VNDA)	An agreement that outlines the administrative, physical and technical mitigation strategies to consider when personal or health information is made accessible to individuals other than clinic employees, and who are providing a specific service to the clinic.