ACTT
Accelerating Change
Transformation Team

Privacy Officer Handbook

Revised March 2023

Table Contents

Disclaimer

This tool is for educational and informational purposes. It is intended to provide guidance and is not a substitute for professional or legal advice. Should you decide to use this tool and its information, you do so at your own risk.

While the information provided in this tool has been produced and/or verified by a team of subject matter experts, it is not guaranteed that it is applicable to every situation, person, or business need.

Introduction

Alberta legislation grants the right to privacy for individuals, and it also outlines a number of requirements that apply to healthcare professionals. This includes designating a clinic privacy officer. The appointment of a designated privacy officer is a key aspect of a clinic's protection of privacy and health information.

The relationship that physicians and their teams have with their patients is based on trust. Your patients trust the clinic team to make the right decisions for their health and they trust the staff to protect their privacy and health information.

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

The clinic privacy officer role is a requirement under the Health Information Regulation Section 8(2)

As the privacy officer for your clinic, you are the "go-to" person for information about Alberta's Health Information Act (HIA). You are responsible for ongoing privacy and security policies and practices, and for emerging privacy and security issues that impact your clinic's operational processes.

- It is vital that everyone in the clinic knows who the privacy officer is in order to direct incoming requests and emerging issues appropriately.
- It is important to note the privacy officer often depends on the Electronic Medical Record (EMR) vendor for many security functions, especially those of a technical nature.

The privacy officer can be a clinic physician or a responsible affiliate (for example, a clinic manager). To be successful in the role of a clinic privacy officer, an individual should have the following important skills:

- An understanding of EMR technology
- Familiarity with privacy principles
- An interest in learning more about privacy requirements and a commitment to staying current
- Knowledge of the clinic's operations
- Rapport with clinic physicians and staff

Privacy Officer Quick 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.
- Privacy training programs are available through the AMA. See the Privacy Training webpage for more details.

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. Additional information is available in the Privacy Officer Advanced Training Curriculum through the AMA. The duties of a privacy officer are divided into four key categories:

A) Develop and keep current privacy policies and procedures	B) Build awareness (training) of Privacy with Clinic staff and vendors	C) Monitor your clinic's ongoing compliance with the Health Information Act	D) Act as the primary point of contact for privacy issues

The specific responsibilities along with additional information and resources are found below.

1) Develop privacy policies and procedures and keep them up to date

Goal: To make sure legislation and clinic policies are being followed.

Tasks	Tips
Develop a process for updating privacy policy information.	The AMA has created 12 policy guidance documents to help you create the most requested policies in your clinic. Set up a reminder for reviewing policies.
Review and stay current with regulatory requirements.	Check out the OIPC website and AMA website on a regular basis.

	Take privacy training for Privacy Officers.
Ensure Doctors, Staff, and Affiliates are aware and have access to Clinic's Privacy/Security Policies/Procedures.	Provide new staff and physicians with all privacy policies when they start at the clinic.
Communicate policy and procedure changes with staff and physicians.	Determine the best way to do this for your clinic, e.g., clinic team meetings.
Resources: • AMA Policy and Procedure resources • AMA Tools and Resources • Privacy training link • Link to the OIPC website	

2) Ensure clinic staff and vendors are aware of their privacy obligations

Goal: To make sure that the key safeguard of staff training is implemented

Tasks	Tips
Coordinate overall privacy training for all staff and physicians in the clinic.	The AMA provides a comprehensive free program. You could consider doing the training as a team.
Track and ensure that privacy training is completed by all staff and physician	Create a tracking form or if you use the AMA training, print out the available report as needed
When necessary, provide training about changes in privacy legislation or changes in clinic policy	Determine the best way to do this for your clinic, e.g., clinic team meetings (five-minute privacy moments), privacy bulletin board, lunch and learns, etc.
Ensure all personnel have access to resources and support	Make sure that they know where to obtain the latest info.
Resources: • Quick Tips: Privacy training for your team • AMA Fundamental Privacy Training	

3) Monitor your clinic's ongoing compliance with the HIA

Goal: Ensure Security and Protection of Health Information in the custody and control of clinic

Tasks	Tips
Implement and review safeguards on a regular basis to protect patient health information	The safeguards are classified as physical, administrative, and technical (PAT). The AMA has created a tool to help review safeguard and create an action plan.
Ensure a disclosure log is implemented and used consistently	The disclosure log must include date, requester name, patient name, information released, method of disclosure and sign off.
Audit EMR logs regularly	Use the handbooks that are available from the EMR vendors. Make sure that you print and review the audit logs. Consider setting up a reminder for yourself.
Post privacy notices (about how your clinic collects Info)	This is a requirement under the HIA. There is an editable template on the AMA website.
Create consent forms and ensure they are utilized appropriately	There is a consent form on the AMA website that you can adapt.
Review confidentiality agreements with staff and Information Manager Agreements with vendors and ensure compliance	Use the template on the AMA website and make sure to keep a copy in a secure location (e.g., personnel files, locked cabinet, electronic folder)
Participate in updating your clinic's PIA with new practice or system changes, that affect collection, use, and disclosure.	Turn your PIA into a tool that you use. Consider offering training about what is in the PIA, or creating a table of the policies contained in the PIA for quick reference.
Always maintain an electronic or paper copy of the clinic PIA(s) in your business records.	Ensure that the PIA is in a well-known location and can be reviewed and updated as needed.

Resources

- Quick Tips: Assessing risks and implementing safeguards
- AMA Privacy and Security Assessment
- Editable privacy notice
- Consent form
- Link to agreements
- Policy table

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

Goal: To ensure that the Health Information Act is being applied correctly

Task	Tip
Be the primary contact for access and disclosure requests, and correction of Information requests.	The AMA Common Questions for Privacy Officers Advanced course is a great resource.
Review patient and client privacy complaints.	Keep a record of the complaints and follow up. This will help you address common issues in the clinic.
Answer questions from physicians and clinic staff.	Make sure you are referencing your clinic's policies and procedures.
In the event of Privacy Breach follow the Breach Management Policy	Download the Quick Tips and Breach Documentation form and have it handy when a breach is suspected

Resources:

- Advanced privacy courses
- Breach management policy
- Quick Tips: Responding to a Privacy Breach
- Breach documentation form

Appendix A: Privacy Breach Management Procedure

A suspected privacy breach must be identified and immediately reported to the clinic privacy officer and clinic manager. The privacy officer initiates the following key steps in responding to a privacy breach:

Step 1: Contain the Breach

- Take immediate steps to stop the breach
- Take corrective action
- Investigate what happened
- Gather information and start the risk assessment

Step 2: Analyze the level of risk and harm to the patient

- What was the cause and extent of the breach?
- Who are the affected individuals?
- What information was involved?
- What is the possible harm?
    - Consider all relevant factors, including those in the Health Information Regulation (section 8.1)

Tool Tip: Find a Risk of Harm checklist within the Breach Management Policy

Step 3: Reporting, notification and follow up based on the level of risk

- Who should or must we notify?
    - Legislated or contractual obligations
    - Risk of harm to affected individuals
- When should or must notification occur?
    - "As soon as practicable" (section 60.1(2) of the HIA)

Step 4: Mitigation to prevent future breaches

- Develop or improve safeguards
    - Review and update policies and procedures, as needed
    - Regularly educate and train staff on safeguards and policies
    - Audit to ensure prevention plan has been implemented

Appendix B: Downloadable Breach Documentation Form

Document Purpose and Overview

The Health Information Act (HIA) states a privacy breach means a loss of, unauthorized access to, or unauthorized disclosure of health information.

This form is intended to guide custodians through the process of addressing a breach including determining the extent of the breach and the potential risk of harm. Please refer to your clinic's Breach Management Policy or to the AMA Breach Management Policy guidance document from the AMA website for further information. If you need additional assistance, you may wish to contact a privacy consultant.

This form can be filled out by the privacy officer but must be signed off by the custodian. The form also serves as a record of the breach and action taken. It should be filed in a secure location to be referenced in the future if needed.

Instructions for use

The instructions below are meant to assist you with making this document your own and to fulfill your obligations under the Health Information Act.

- This form can be filled out by the privacy officer but must be signed off by the custodian.
- The form also serves as a record of the breach and action taken. It should be filed in a secure location to be referenced in the future if needed.
- **Patient names should not be included in the information shared to OIPC or the Minister. This documentation is for your information only and you must fill out the appropriate reporting forms for OIPC and the Minister.**

Breach Documentation Form

Part A. Breach Information

Complete the section below to conduct a full assessment of the breach that has occurred. It is important to assess all elements of the breach as this will help you to determine the risk of harm and the need to report the breach. It's important to include your rationale in the sections provided because you may need to refer to this information in the future.

Name of person filling out the form:	Date:

	Yes	No	
Privacy Officer informed:	☐	☐	Privacy Officer name:
Key physicians involved informed:	☐	☐	Lead clinic physician name:

Describe how the breach was discovered. Who were the key staff and physicians involved in the breach and what was their role?

Was the cause of the breach a loss of information **OR** unauthorized access **OR** unauthorized disclosure? Describe your reasoning below.

List the types of health information involved. Health Information includes diagnostic, treatment and care information or registration information. This pertains to #11 on the OIPC privacy breach reporting form. Do not include individually identifying information.

When did the breach occur? When was it discovered?

Whose information has been breached?
If the information has been disclosed, how wide is the spread of information? Please describe below.

Part B. Risk of Harm

The Health Information Regulation defines the factors custodians must consider when assessing the risk of harm. This checklist can be used to assist the custodian and privacy officer to ensure all factors were considered.

RISK OF HARM CONSIDERATIONS	Yes	No	ASSESSMENT RATIONALE
Is there reason to believe that the information has been or may be accessed by or disclosed to an unauthorized individual?	☐	☐	
Is there a reason to believe that the information has been or will be used for malicious purposes (intentional or not)?	☐	☐	
Is there a reason to believe that the information could be used for the purpose of identity theft or to commit fraud?	☐	☐	
Is there a reason to believe that the information involved in the breach could cause: • Embarrassment • Physical, mental, or financial harm • Damage of reputation	☐	☐	
Is there a reason to believe that the breach has or may adversely affect the provision	☐	☐	

of a health services to the individual?			
Are there any other factors that indicate a risk of harm to the affected individual?	□	□	
*If you answer "YES" to any of the questions, please continue on to Section C to ensure that the breach was not mitigated before notice under Section 60.1(2) of the HIA. *If you answer "NO" to all the questions then the breach may not be reportable.			

Part C. Mitigation Factors

There are mitigating factors that a custodian must consider in reporting a breach. Complete the section (s) that is applicable to your type of breach.

	Yes	No
1. For loss of information:		
• Was the electronic information encrypted or otherwise secured in a manner that would prevent the information from being accessed or make the information useless?	□	□
• Do you have confirmation the information was destroyed or made useless?	□	□
• If it was recovered, is there confirmation that it was not accessed before it was recovered?	□	□
• If it was recovered, is there confirmation that the information was only viewed to determine that the information was provided in error?	□	□
2. For unauthorized access of information, can the custodian demonstrate that the person:		
• Is a custodian or an affiliate?	□	□
• Is subject to a confidentiality agreement and HIA compliant policies and procedures?	□	□
• Accessed the information in a manner that is relevant to the person's duties?	□	□
• Was not inappropriately accessing information? (i.e., snooping)	□	□
• Did not use the information except in determining that the information was accessed in error, and steps have been taken to address the error?	□	□
3. For unauthorized disclosure of information, can the custodian demonstrate:		

• That the information was disclosed to a custodian or an affiliate?	☐	☐
• That the recipient was subject to a confidentiality agreement and HIA compliant policies and procedures?	☐	☐
• That the person disclosing the information had the authority to do so?	☐	☐
A custodian may decide that notification is necessary even when mitigating factors are present. Each situation is unique, and all factors should be considered.		

Part D. Reporting and Mitigation:

The custodian must report the breach unless they are able to demonstrate the breach was mitigated and there was no risk of harm. Use the checklist below to document your reporting and attach the forms sent to the various parties.

Did the custodian report the breach?	**Yes**	**No**	**Date (if applicable)**
Notified OIPC using OIPC privacy breach reporting form	☐	☐	
Notified Minister of Health using AH Minister reporting form	☐	☐	
Notified the patient using patient notification letter template	☐	☐	

Mitigation and Remediation Notes

Describe any steps that the custodian has taken or is intending to take, to reduce the risk of harm to the individual(s) involved in this breach.
Describe any steps that the custodian has taken or is intending to take, to reduce the risk of future breaches.

Custodian Signature:	Date:

Appendix C: Privacy & Security Risk Assessment

Privacy and security risk assessments are conducted by clinics to determine if there are gaps in a clinic's privacy and security policies, practices and procedures. It will help fulfil the custodians' obligations under the Alberta Health Information Act (HIA) to periodically ensure that proper safeguards for protecting information are in place.

Objectives

The purpose of the privacy and security risk assessments are to:

- **Enable** a clinic to analyze its privacy and security policies, procedures and practices.
- **Identify** privacy and/or security risks and determine if clinic controls are in place to mitigate those risks.
- **Develop and implement** privacy and security improvements and controls where necessary to reduce clinic privacy and security risks.

How to Use the Tool

This tool presents a series of risks and questions that will help the clinic determine if key privacy risks are being addressed. The risks are organized under:

- **Physical Environment Risks & Physical Safeguards**
- **People Risks & Administrative Safeguards**
- **Technology Risks & Technical Safeguards**

Guidance about what risk you are assessing and mitigating are provided in each section. This tool will assist you in developing a plan to help ensure that appropriate safeguards are in place. It is recommended that you keep or save the completed tool in a safe place as it provides documentation that the risk assessment was completed and the action plan that was created. This privacy and security risk assessment is intended to be completed on a regular basis (e.g., annually).

Part A. Physical Environment Risks & Physical Safeguards

Name: _____ **Date:** _____

Privacy Risk		Safeguard Considerations	Yes	No	Suggested Resources
1	**Errors in information handling and compliance with legislation**	Does the clinic have a process for verifying the identity of patients?	☐	☐	Collection, use and disclosure policy
		Is there written documentation that identifies the clinic's purpose for collecting health information, authority to collect and who to contact regarding privacy concerns?	☐	☐	Notification of Collection of Health Information Poster
		Does the clinic have a process for verifying the identity of contractors and their employees, vendors and couriers?	☐	☐	Information Security in Contracting Policy
2	**Information could be lost and misused**	Are servers, computers, laptops and smartphones with EMR access to patient health information reasonably secured to prevent theft?	☐	☐	
		Are fire extinguishers, smoke detectors, deadbolt locks and other general security items in place?	☐	☐	Information Handling Policy
3	**Information could be accessed by people without authority**	Are there policies and procedures in place for securing patient health information?	☐	☐	Information Handling Policy
		Are there policies and procedures for the retention and secure destruction of health information?	☐	☐	Information Handling Policy
		Are patient records in paper format secured away from public access within the clinic?	☐	☐	Information Handling Policy
		Are wireless routers stored away from easily accessible areas?	☐	☐	Information Handling Policy
		Does the clinic have a list of people with authorized access (e.g., key FOBs, door keys, alarm passcodes, swipe cards) and is it updated regularly?	☐	☐	Information Handling Policy
		Does each authorized staff member have their own alarm code?	☐	☐	
		Does the clinic have an intrusion system (e.g., monitoring noise/motion, alarms, automated response, other theft prevention measures)?	☐	☐	

Privacy Risk		Safeguard Considerations	Yes	No	Suggested Resources
		Are the clinic locks and alarms regularly tested to ensure they are working properly and are the security company contact lists up to date?	☐	☐	
4	**Information could be disclosed and misused**	Are strategies used to reduce people overhearing confidential information within the clinic (e.g., radio or television in the waiting room, white noise)?	☐	☐	Information Handling Policy
		Are clinic fax machines and printers located in a secure area away from public view and access?	☐	☐	Fax Transmission Guidelines Information Handling Policy
		Is a written 'if received in error' notification included on all clinic fax cover sheets and emails?	☐	☐	Email Guidelines Fax Transmission Guidelines

Physical Environment Risks & Physical Safeguards Action Plan

Review the items that have a 'No' in the section above and determine if any processes or procedures could be improved. To fill out the form below, first identify the type of risk then list the safeguards needed, based on the 'No' answers. Once your missing safeguards are listed, develop an action plan with timelines and who is responsible to ensure that the issue is addressed. This action plan should be based on priority and high-risk areas need to be addressed first.

Risk #	Safeguards Needed	Action Plan	Responsible	By When
		•		
		•		
		•		
		•		

Part B. People Risks & Administrative Safeguards

Name: _____ **Date:** _____

Privacy Risk		Safeguard Considerations	Yes	No	Suggested Resources
1.	**Errors in information handling and compliance with legislation**	Has an individual(s) been designated as the privacy officer?	☐	☐	Privacy Officer Handbook
		Is there an individual responsible for addressing and responding to patient privacy complaints?	☐	☐	Privacy Officer Handbook
		Does the clinic have established and implemented policies and procedures in place for protecting health information as required under the Health Information Act (HIA)?	☐	☐	Policies and Procedures Table
		Are policies and procedures regularly reviewed and updated?	☐	☐	
		Do clinic staff members receive regular privacy training including HIA and cybersecurity training?	☐	☐	AMA privacy training
		Is there a breach management process in place that reflects mandatory breach reporting? Is it reviewed annually?	☐	☐	Privacy Breach Management Policy
		Is there a process that enables patients to request updates or corrections to health information?	☐	☐	Correction or Amendment of Health Information Policy
		Is there a process for patients to request access to their health information?	☐	☐	Right of Access Policy
		Does the clinic maintain a record of disclosures containing all relevant details for each information request?	☐	☐	Information Handling Policy
		Is written consent obtained from patients when health information is disclosed as outlined in the HIA? (when required)	☐	☐	Release of Information and Disclosure Process Consent form
		Are there policies and procedures that mandate the safeguarding of health information by all clinic staff?	☐	☐	Information Handling Policy

Privacy Risk		Safeguard Considerations	Yes	No	Suggested Resources
		Is there a policy for handling patient information in a consistent manner?	☐	☐	Information Handling Policy
		Is there an Internet usage policy?	☐	☐	Information Handling Policy
2.	**Information could be lost and misused**	Is an Information Management Agreement (IMA) in place for any third-party vendor that has access to patient information?	☐	☐	IMA template
		Do vendors and contractors (e.g., cleaners, maintenance) sign a non-disclosure/confidentiality agreement?	☐	☐	Information Security in Contracting Policy Non-Disclosure Agreement
3.	**Information could be accessed by people without authority**	Is there a new hire checklist that covers access controls?	☐	☐	
		Is there a checklist for when employees leave that covers removing access controls and returning equipment?	☐	☐	
4.	**Information could be disclosed and misused**	Have all affiliates signed an oath of confidentiality and are they updated annually?	☐	☐	Oath of Confidentiality

People Risks & Administrative Safeguards Action Plan

Review the items that have a 'No' in the section above and determine if any processes or procedures could be improved. To fill out the form below, first identify the type of risk then list the safeguards needed, based on the 'No' answers. Once your missing safeguards are listed, develop an action plan with timelines and who is responsible to ensure that the issue is addressed. This action plan should be based on priority and high-risk areas need to be addressed first.

Risk #	Safeguard Needed	Action Plan	Responsible	By When
		•		
		•		
		•		
		•		

Part C: Technology Risks & Technical Safeguards

Name: _____ **Date:** _____

Privacy Risk		Safeguards Considerations	Yes	No	Suggested Resources
1	**Errors in information handling and compliance with legislation**	Does the clinic back up non-EMR data such as personnel files and email?	☐	☐	Information Handling Policy
2	**Information could be accessed by external people without authority**	Does a password-protected screensaver automatically display after the computer has been idle for a reasonable period of time, given where the computer is located in the clinic?	☐	☐	Information Handling Policy
		Does everyone lock their computer (e.g., "ctrl-alt-del" key combination) if it's unattended?	☐	☐	Information Handling Policy
		Does the EMR automatically log off the user if it has been idle for more than a reasonable period of time?	☐	☐	Information Handling Policy
		Is dual authentication required for logging in?	☐	☐	Information Handling Policy
		Are computer hard drives set up with encryption?	☐	☐	Information Handling Policy
		Is the clinic using a known anti-virus or anti-spyware software? Is the software updated automatically?	☐	☐	Information Handling Policy
		Is the computer operating system updated regularly?	☐	☐	
		Is the wireless network encrypted with tools such as Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access II (WPA2)?	☐	☐	Wireless Networking and Remote Access Policy
		Is a secure wireless channel utilized if a clinic laptop is used outside of the clinic?	☐	☐	Wireless Networking and Remote Access Policy
		Is everyone required to change their passwords every 90 days for access to clinic computers, EMR and Alberta Netcare?	☐	☐	Wireless Networking and Remote Access Policy Password Guidelines

Privacy Risk		Safeguards Considerations	Yes	No	Suggested Resources
		Are password standards enforced in the EMR solution and clinic computers?	☐	☐	Wireless Networking and Remote Access Policy Password Guidelines
		Are there established policies and procedures regarding the transmission of health information via email?	☐	☐	Email Acceptable Use Guidelines
3	**Information could be accessed by internal people without authority**	Are audit logs completed regularly, reviewed and documented?	☐	☐	Information Handling Policy
		Is everyone assigned a unique user ID and aware not to share IDs and passwords for EMR access?	☐	☐	Password Guidelines
		Are staff assigned appropriate user access rights for the EMR and computer network?	☐	☐	Information Handling Policy

Technology Risks & Technical Safeguards Action Plan

Review the items that have a 'No' in the section above and determine if any processes or procedures could be improved. To fill out the form below, first identify the type of risk then list the safeguards needed, based on the 'No' answers. Once your missing safeguards are listed, develop an action plan with timelines and who is responsible to ensure that the issue is addressed. This action plan should be based on priority and high-risk areas need to be addressed first.

Risks #	Safeguard Needed	Action Plan	Responsible	By When
		•		
		•		
		•		
		•		

Appendix D – Key policies needed for the Clinic

Topic Requiring a Policy	Recommended AMA Policy Resource Document
Privacy Accountability	Privacy Charter
Health Information and Privacy Practices	Privacy Roles and Responsibilities Policy Guidance Document
Access to Health Information	Right of Access Policy Guidance Document
Correction Requests	Correction or Amendment of Health Information Policy Guidance Document
Training, Awareness & Sanctions	Information Handling Policy Guidance Document
Collection of Health Information	Collection Use, Disclosure and Disposal of Health Information Policy Guidance Document
Use of Health Information	Collection, Use, Disclosure and Disposal of Health Information Policy Guidance Document
Disclosure of Health Information	Collection, Use, Disclosure and Disposal of Health Information Policy Guidance Document
Research	
Third Parties	Information Security for Contractors Policy Guidance Document
Privacy Impact Assessments	Privacy Roles and Responsibilities Policy Guidance Document
Records Retention & Disposition	Collection, Use, Disclosure and Disposal of Health Information Policy Guidance Document
Information Classification	
Risk Assessment	Privacy and Security Risk Assessment Checklist
Physical Security of Data and Equipment	Information Handling Policy Guidance Document
Network & Communications Security	Wireless Networking and Remote Access Policy Guidance Email acceptable use Policy Guidance Document Facsimile Transmission Guidelines Password guidelines
Monitoring and Audit	Access Control Chart
Incident Response	Privacy Breach Management Policy Guidance Document
Business Continuity	Information Handling Policy Guidance Document

Information Flow and Legal Authorities	Information Flow and Legal Authorities Sample
Mandatory Breach Reporting	Privacy Breach Management Policy Guidance Document

Appendix E: Responding to a Request for Information

Here are the steps to follow when a patient or representative requests their information. The steps are all required, but they may occur in a different order, depending on the clinic's internal processes. All requests should be obtained in writing with the patient's signature.

Step 1:

Read the request. The request should contain:

- Name, address and date of birth
- Specific information being asked for during a defined time period.

Step 2:

Discuss the request with the custodian and determine how to proceed with the request.

Step 3:

Print the relevant sections of the record.

Step 4:

Redact or remove information that:

- Was not specifically requested such an information about additional diagnoses
- Could cause harm to the patient or physician if it was disclosed such as an inappropriate comment or information related to another person

Step 5:

Obtain a sign off by the custodian of the record. Some custodians may prefer to sign off at step 2.

Step 6:

Collect the fees outlined in the regulations if applicable

Step 7:

Provide the information to the patient. Remember this process must be completed within 30 days.

Appendix F: Printable Clinic Privacy Officer Tasks Checklist

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.			✔
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, administration, practices, staffing, physical security, orientation, etc.	✔		✔

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.	✔		
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 external 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 Clinic Privacy and Security Program 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.	✔		
Consider the need to update the clinic's PIA periodically 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 vendors).		✔	✔
Ensure a disclosure log is implemented and used consistently.	✔		✔
Determine if an Information Sharing Agreement (IMA) is necessary (usually required when there is more than one physician at a location).	✔		✔
Protect clinic staff personal information according to the Freedom of Information and Protection of Privacy Act (FOIP) and 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 that process, store, retrieve or dispose of health information review and execute an Information Manager Agreement.	✔		✔
Oversee the selection, testing, deployment and maintenance of security hardware and software products.	✔		✔
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.	✔		✔
For any incident/breach use the Risk of Harm checklist within the Breach Management Policy.			✔
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.			✔

Primary Point of Contact for Privacy-Inquiries	Initial	Annual	Ongoing
Act as the clinic primary contact in regard to the HIA and clinic privacy and security policies.			
Be familiar with obligations under the HIA.	✔		✔
Make yourself known to the physicians and staff as the primary privacy clinic resource.	✔		✔
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.			✔
Act as the main point of contact in dealings with third parties (Alberta Medical Association, 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 with regards to the clinic's collection, use and disclosure of or access to health information.			
Use the Chapter 14 Duty to Notify Health Information Act 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.			✔
Document each privacy breach or suspected privacy breach, its investigation, recommendations and lessons learned.			✔

Appendix G: 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
2021-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

Appendix H: Privacy Resources

- Health Information Act: Guidelines and practices manual (2011)
- Health Information Act guidelines and practices manual Chapter 15: 2020 amendments (April 2021)
- Health Information Act Guidelines and Practices Manual: Duty to Notify; Chapter 14 (August 2018)
- Health Information: A Personal Matter – A Practical Guide to the Health Information Act (OIPC)
- Alberta Medical Association's privacy training

Important Contacts

Stakeholders and Authorities	For Assistance With
Alberta Netcare Provincial Service Desk Local: 780.412.6778 Toll Free: 877.931.1638 Hours: 24/7	• Netcare technical issues • Password resets including AHS IAM for community users
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
eHealth Netcare Support Services Team Toll Free: 855.643.8649 Email: ehealthsupport@cgi.com Hours: 8:15 a.m. - 4:30 p.m.	• Access & Registration User Training • Privacy & Security Services • Student Education Program
RSA Token Support Toll Free: 844.542.7876	• To report lost/stolen token • Setup/configuration of token ID or hard/soft token • To return your token

Health Information Act (HIA) Help Desk Local: 780.427.8089 (Toll free in Alberta 310.0000) Email: **HiaHelpDesk@gov.ab.ca** Hours: 8:15 a.m. - 4:30 p.m. Monday - Friday	• Questions about the Health Information Act (HIA) or your responsibility as an Alberta health care provider.
College of Physicians & Surgeons of Alberta Website: College of Physicians & Surgeons of Alberta | CPSA General inquiries: 1.800.561.3899 Questions about billing or PracIDs 780.422.1522 Alberta Health Facilities & Clinics - College of Physicians & Surgeons of Alberta | CPSA Standards of Practice - College of Physicians & Surgeons of Alberta | CPSA Resources - College of Physicians & Surgeons of Alberta | CPSA	• Privacy issues involving physicians, ownership of patient records or patient records retention Facility Accreditation Standards of Practice Privacy Resources

Appendix I: 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
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.
Collect	To gather, acquire, receive, or obtain health information. Source: Health Information Act
Consent	An individual giving permission to have their 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:

Term	Definition
	• Physicians & surgeons • Pharmacists • Optometrists • Opticians • Chiropractors • Midwives • Podiatrists • Denturists • Ambulance operators • Registered nurses • Dentists and dental hygienists • Hospital boards • Alberta Health Source: Health Information Act
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: diagnostic, treatment and care information; registration information. Source: Health Information Act
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:

Term	Definition
	• Processes, stores, retrieves or disposes of health information. • Strips, encodes or otherwise transform 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) Information Manager Agreement (IMA)	A legislative requirement when a custodian hires an information manager. The agreement 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 and Health Information Regulation
Information Sharing Agreement (ISA)	In the context of EMR implementations, the legal contract between clinic organizations and EMR vendors that

Term	Definition
	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)

Term	Definition
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 (FOIP 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. 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. PIAs assist custodians in reviewing the impact that new programs, systems and practices may have on individual patient privacy and

Term	Definition
	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, drawings, 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
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