Privacy Self-Assessment

**Table of Contents**

[Introduction 1](#_Toc410897588)

[Objectives 1](#_Toc410897589)

[Approach 1](#_Toc410897590)

[Answering the Self-Assessment Questions 1](#_Toc410897591)

[Privacy Self-Assessment Questions 2](#_Toc410897592)

[Management 2](#_Toc410897593)

[Privacy Notifications 3](#_Toc410897594)

[Consent 4](#_Toc410897595)

[Collection 6](#_Toc410897596)

[Use, Retention and Disposal 6](#_Toc410897597)

[Accuracy 7](#_Toc410897598)

[Disclosure to Third Parties 7](#_Toc410897599)

[Safeguards 8](#_Toc410897600)

[Access 10](#_Toc410897601)

[Monitoring and Compliance 10](#_Toc410897602)

[Privacy Modifications and Improvements 12](#_Toc410897603)

[Action Plan 12](#_Toc410897604)

[Questionnaire Interviewees 12](#_Toc410897605)

The information in this assessment 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.

# Introduction

Privacy self-assessments are conducted by clinics to determine if there are gaps in a clinic’s privacy policies, practices and procedures.

## Objectives

The purpose of the privacy self-assessment is to:

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

## Approach

The privacy self-assessment is used as an evaluation tool to help clinics review privacy policies and practices annually and identify areas for improvement.

The questions can be answered in two ways:

1. Answer the assessment questions based on an understanding of how processes within the clinic operate without providing or confirming the existence of documentation of the process, but by describing the procedure in effect at the clinic.

For example, one question asks the following: “Does the clinic have established policies and procedures that mandate the safeguarding of personal information by all clinic staff?” The clinic may respond to this question by indicating that the procedure in place requires support staff to shut off their computers at the end of each workday. No documentation needs to be provided to confirm this practice within the clinic.

1. Answer the assessment questions based on an understanding of how processes within the clinic operate and provide documentation of the process within the clinic.

For example, one question asks the following: “Does the clinic have established policies and procedures that mandate the safeguarding of personal information by all clinic staff?” The clinic may respond to this question by referencing the existence of a checklist that is completed each night by the clinic manager verifying that all computers have been shut off at the end of a workday.

The first approach helps clinics gain a general idea of the privacy policies and practices implemented within the clinic. This helps the clinic identify areas for improvement and areas that require more stringent privacy measures.

The second approach provides the clinic with confirmation that privacy policies and procedures in the checklist are implemented within the clinic and are being followed consistently.

## Answering the Self-Assessment Questions

The Privacy Self-Assessment Questions in the following table can be answered by clicking in the available fields. Entered content can be saved in Acrobat Reader using the File > Save As command which enables you to save your current answers and reopen your assessment to complete it at a later time.

# Privacy Self-Assessment Questions

The following questions are categorized by the type of privacy the questions address.

1. In the “How is it confirmed that the policy or procedure is operating in the clinic?” column, identify what evidence is available to confirm that the policy and or procedure is currently operating in the clinic.
2. In the “Reference the name of the policy or procedure that answers the question” column, identify the name of the clinic policy or procedure that addresses or answers the question.

| **Questions** | | **1. How is it confirmed that the policy or procedure  is operating in the clinic?** | **2. Reference the name of the policy or procedure that answers the question** | **Notes and comments** |
| --- | --- | --- | --- | --- |
| Management | | | | |
| 1. Does the clinic custodian accept responsibility for the health information under their control? | **Y**  **N** |  |  |  |
| 1. Has one individual been designated or made accountable for the clinic’s overall compliance with the *Health Information Act* (HIA)? 2. Is this individual designated as the clinic’s privacy officer? 3. Who is this individual? 4. Has this individual been provided with initial and ongoing privacy training (e.g., courses or online training)? | **Y**  **N** |  |  |  |
| 1. Does the clinic use contracts, Information Manager Agreements or other means to ensure a comparable level of protection while information is with a third party for processing? | **Y**  **N** |  |  |  |
| 1. Does the clinic have established and implemented policies and procedures in place for protecting health information as required under the HIA? | **Y**  **N** |  |  |  |
| 1. Does the clinic have established policies and procedures for receiving and responding to privacy complaints and inquiries? | **Y**  **N** |  |  |  |
| 1. Are policies and procedures reviewed and updated on a regular basis? | **Y**  **N** |  |  |  |
| 1. Do clinic staff members receive regular training and refreshers on maintaining the privacy of health information and the proper handling of health information? | **Y**  **N** |  |  |  |
| 1. Has the clinic determined the potential risks involved with maintaining health information and planned the mitigation strategies for those risks? | **Y**  **N** |  |  |  |
| Privacy Notifications | | | | |
| 1. Is there written documentation that identifies the clinic’s purpose for collecting health information? | **Y**  **N** |  |  |  |
| 1. Is written notice provided to your patients identifying the purposes for which health information is collected, used, retained and disclosed? | **Y**  **N** |  |  |  |
| 1. Is written notice provided to your patients about the privacy policies and procedures that are currently implemented in the clinic? | **Y**  **N** |  |  |  |
| 1. Is a written “if received in error” notification included on all clinic faxes and emails? | **Y**  **N** |  |  |  |
| Consent | | | | |
| 1. Is written consent obtained from patients when health information is disclosed by the physician to a person other than the individual who is the subject of the information for purposes that are not listed in section 27(1) or (2) of the HIA? | **Y**  **N** |  |  |  |
| **Sections 27(1) and (2) of the HIA) state:**  Physicians can disclose health information without individuals' consent to Alberta Health or the provincial health authority for the following purposes:   * providing health services; * determining or verifying the eligibility of an individual to receive a health service; * conducting investigations, discipline proceedings, practice reviews or inspections relating to the members of a health profession or health discipline; * conducting research or performing data matching (Note: HIA has additional requirements for research and or data matching); * providing for health services provider education; * carrying out any purpose authorized by an enactment of Alberta or Canada; * for internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management.   In addition, physicians can disclose health information without individuals' consent to Alberta Health or the applicable local health authority in support of their mandate to manage public health. | | | | |
| 1. If YES is answered to question 13, is the following information included in the consent form? 2. Authorization for the custodian to disclose health information specified in the consent? 3. Purpose for which the health information is being disclosed? 4. Identity of the person to whom health information may be disclosed? 5. Acknowledgment that the individual providing the consent is aware of the reasons why health information is needed? 6. Date consent is effective and date when consent expires? 7. Statement indicating consent may be revoked at any time by individual providing it? | **Y**  **N**  **Y**  **N**  **Y**  **N**  **Y**  **N**  **Y**  **N**  **Y**  **N** |  |  |  |
| 1. Is written notice provided to patients about the implied consent that is given when patients provide health information to a physician or clinic staff member? | **Y**  **N** |  |  |  |
| 1. If health information is being collected from a patient using a recording device or camera or any other device that may not be obvious to the individual, is written consent obtained from the individual to use said device or camera? | **Y**  **N** |  |  |  |
| Collection | | | | |
| 1. Is written notice provided to patients about how their health information will be collected? | **Y**  **N** |  |  |  |
| 1. What practices are currently in place to ensure documents collected from a patient are handled properly to maintain the privacy of the information provided? | **Y**  **N** |  |  |  |
| Use, Retention and Disposal[[1]](#footnote-1) | | | | |
| 1. Does the clinic have established policies and procedures that mandate the acceptable use of health information? | **Y**  **N** |  |  |  |
| 1. Does the clinic have established policies and procedures in place that mandate the required retention of health information? | **Y**  **N** |  |  |  |
| 1. Does the retention policy identify the maximum and minimum periods for retention? | **Y**  **N** |  |  |  |
| 1. If the clinic accepts point of sale debit cards or credit cards, are policies and procedures for receipt storage methods and retention periods in place? | **Y**  **N** |  |  |  |
| 1. Are established policies and procedures in place that govern the clinic’s secure destruction of health information, including transitory records (phone messages or sticky notes)? | **Y**  **N** |  |  |  |
| 1. Does the clinic have established policies and procedures in place that govern the secure destruction of electronic storage devices (e.g., CDs, hard drives, fax machine memory)? | **Y**  **N** |  |  |  |
| 1. Does the clinic record the secure destruction of health information and electronic storage devices? | **Y**  **N** |  |  |  |
| Accuracy | | | | |
| 1. Does the clinic have an established policy or procedure that enables its patients to request updates or corrections to health information? | **Y**  **N** |  |  |  |
| 1. Does the clinic have an established policy or procedure to ensure that information is reviewed for accuracy prior to being disclosed? | **Y**  **N** |  |  |  |
| Disclosure to Third Parties | | | | |
| 1. Does the clinic require contractors and vendors to sign and agree to an Information Manager Agreement (IMA) when obtaining information manager services? | **Y**  **N** |  |  |  |
| 1. Does the clinic require affiliates who may have access to patient health information to sign oaths of confidentiality? | **Y**  **N** |  |  |  |
| 1. Does the clinic use contractual or other means to ensure third parties protect health information from loss, misuse, unauthorized access, disclosure, alteration and destruction? | **Y**  **N** |  |  |  |
| 1. Do agreements with third parties establish remedial action the clinic can take in response to misuse of health information by the third party? | **Y**  **N** |  |  |  |
| 1. Does the clinic provide written notice to patients about the disclosure of health information to third parties and the purposes for such disclosures? | **Y**  **N** |  |  |  |
| 1. Does the clinic maintain a disclosure log containing all relevant details for each information request? | **Y**  **N** |  |  |  |
| 1. What steps does the clinic perform to process access requests? Who processes the request, verifies the requesting party, and manages fees and response timelines? | **Y**  **N** |  |  |  |
| 1. Does the clinic have documentation outlining when information (as detailed in the HIA):  * Can be disclosed? * Cannot be disclosed? * Must be disclosed? * Must not be disclosed? | **Y**  **N** |  |  |  |
| Safeguards | | | | |
| 1. Does the clinic have established policies and procedures that mandate the safeguarding of health information by all clinic staff? | **Y**  **N** |  |  |  |
| 1. Does the clinic record patients’ expressed wishes and review them prior to any disclosures of information (e.g., minor on birth control who doesn’t want her parents to know)? | **Y**  **N** |  |  |  |
| 1. Does the clinic have established procedures requiring clinic staff to obtain proper approvals prior to be given access to patient health information? | **Y**  **N** |  |  |  |
| 1. Does the clinic have established procedures to ensure computers and laptops with EMR access or patient health information are properly secured to prevent theft? | **Y**  **N** |  |  |  |
| 1. Does the clinic have established policies and procedures for properly securing patient health information during storage? | **Y**  **N** |  |  |  |
| 1. Does the clinic have established policies and procedures that restrict the transmission of patient health information in email? | **Y**  **N** |  |  |  |
| 1. Does the clinic have established policies and procedures for identifying copies of information given out (e.g., using a “copy” stamp)? Does the clinic record all disclosures, and if so, how and where? | **Y**  **N** |  |  |  |
| 1. Does the clinic have established policies and procedures for verifying the identity of patients, third-party vendor employees and couriers? | **Y**  **N** |  |  |  |
| 1. Does the clinic have an alarm system? Who has the pass codes to this alarm system? | **Y**  **N** |  |  |  |
| 1. Are clinic facilities reviewed on a regular basis to ensure safeguards within the clinic are working properly? How frequently do these reviews take place? | **Y**  **N** |  |  |  |
| 1. Does the clinic have mitigation strategies to limit the overhearing of health information within the clinic (e.g., radio or television in the waiting room, walls that protect physician-patient conversations)? | **Y**  **N** |  |  |  |
| 1. If the clinic and physicians engage in research, are there policies and procedures in place that keep patient information confidential? What steps have been taken to gain approval for the research project? | **Y**  **N** |  |  |  |
| Access | | | | |
| 1. Does the clinic have established procedures in place to enable patients to access their health information? | **Y**  **N** |  |  |  |
| Monitoring and Compliance | | | | |
| 1. Does the clinic monitor ongoing compliance with privacy policies, procedures and practices? How is this accomplished? | **Y**  **N** |  |  |  |
| 1. Are security policies currently monitored and enforced in the clinic? How is this accomplished? | **Y**  **N** |  |  |  |
| 1. Are staff members, volunteers and third-party vendors required to sign a Confidentiality Oath with the clinic? Are oaths updated annually? | **Y**  **N** |  |  |  |
| 1. Are audit logs in the clinic EMR reviewed? Who conducts these reviews? What is the frequency of these reviews? | **Y**  **N** |  |  |  |
| 1. If the clinic is using Netcare, are audit logs in Netcare being reviewed? Who conducts these reviews? What is the frequency of these reviews? | **Y**  **N** |  |  |  |
| 1. Is there an individual within the clinic who is responsible for addressing and responding to patient privacy complaints? | **Y**  **N** |  |  |  |
| 1. Is written or verbal notice provided to patients detailing who they can contact should they have privacy concerns or questions? | **Y**  **N** |  |  |  |
| 1. Does the clinic have an established privacy breach management process in place? Is it reviewed annually? | **Y**  **N** |  |  |  |

# Privacy Modifications and Improvements

When the Privacy Self-Assessment questions are complete, it’s important to review your answers and determine if any security processes and procedures are being overlooked in your clinic.

Identify the processes and procedures that need to be implemented and develop an action plan that addresses when and how they can be made operational. This action plan should be based on priority.

Some considerations in developing these modifications and improvements include but are not limited to:

* Any urgent or high-risk areas of concern which need to be addressed immediately
* Processes and procedures that can be improved within the clinic to strengthen privacy controls
* Regularly scheduled reviews of clinic privacy policies and procedures
* Any upcoming clinic changes that will affect clinic privacy policies and procedures that need to be addressed

## 

## Action Plan

|  |  |  |  |
| --- | --- | --- | --- |
| **Issue** | **Action** | **Date and Time** | **Responsible Party** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## Questionnaire Interviewees

|  |  |  |
| --- | --- | --- |
| **Interviewees** | **Date and Time** | **Location and Role** |
|  |  |  |
|  |  |  |
|  |  |  |

1. “Disposal” may also be referred to as “disposition.” [↑](#footnote-ref-1)