# Information Handling Policy

# Policy Details

Creation date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Revision date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Applies to: All employees and contractors

Approved by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Purpose

The information security provisions of the Health Information Act (HIA) require custodians to protect personal health information in its custody or control by making reasonable efforts to protect against unauthorized access, collection, use, disclosure, or destruction. This policy outlines administrative, technical and physical safeguards to protect health information.

## Scope

This policy applies to:

* Clinic custodians, affiliates, volunteers, and contractors providing services on behalf of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
* Records in any form created or received while carrying out the clinic functions and activities
* All facilities and equipment involved in handling health or personal information

## Physical Safeguards

The section below provides you with the items that should be covered in your policy and prompts you to provide details on how these safeguards would function in your clinic and the role responsible for the activities. Please review the items and adapt these to describe the safeguards in your clinic.

* All CLINIC NAME records, both on-site and off-site, are held and stored in a safe, and secure manner in accordance with information security standards. (Please describe how they are held and secured E.g., locked file cabinet, locked room, secure offsite location, etc.)
* All servers and equipment storing health information are secured by locked cabinets or locked room within CLINIC NAME when not under direct supervision.
* Where confidential paper with patient information is stored, areas are equipped with smoke detectors and fire extinguishers. (If Applicable)
* The clinic follows these practices for file handling while the clinic is open: (always in a closed folder, never left unattended, only certain staff have access, etc.). Please provide details of how this is done in your clinic.
* The computer screens are positioned to reduce the potential of unauthorized access to information by ensuring patients can’t see other people’s health information. Please provide specific details about how and when this is done in your clinic to prevent patients from seeing other people’s information.
* Provide the clinic’s policy on removable media, such as hard drives or thumb drives, if applicable. For example, all removable media devices are encrypted, or must be signed out of the clinic, etc.
* Before CLINIC NAME custodian or staff member is granted off-site access to CLINIC NAME information system, the custodian or staff member obtains approval from the Privacy Officer.
* A staff member will accompany patients and visitors to private or semi-private clinic areas such as examination rooms and physicians’ offices. It is not required that a staff member waits with them in the room or office.
* Confidential information is not transmitted verbally if conversations can be overheard or intercepted.
* Confidential, restricted, or sensitive information that is transmitted by mail or courier is sealed, marked as confidential, and directed to the attention of the authorized recipient.
* CLINIC NAME staff verify the identity and credentials of courier services used for the transportation of personal health information.
* Fax machines and printers that may be used to send or receive confidential information are located in a secure area. Please refer to the Fax Transmission Policy for CLINIC NAME.
* The clinic tracks who have access to codes, keys, fobs and company electronic equipment. Please provide details about how this is done (E.g., a spreadsheet is kept up to date by the office manager).
* The clinic has hiring and termination processes that includes assigning and revoking access codes, keys, fobs, etc. Please describe the process.

## Administrative Safeguards

The section below provides you with the items that should be covered in your policy and prompts you to provide details on how these safeguards would function in your clinic and the role responsible for the activities. Please review the items and adapt these to describe the safeguards in your clinic.

* All CLINIC NAME custodians, affiliates, volunteers, and contracted personnel that collect, use, disclose or have access to confidential information as part of the performance of their duties for CLINIC NAME will sign a Confidentiality Agreement.
* Custodians, affiliates, volunteers, and contracted personnel will review and sign a confidentiality agreement or non-disclosure agreement \_\_\_\_\_\_\_\_\_\_\_\_ (how often will it be reviewed in your clinic)
* Regular audit logs are performed to ensure that information is not being accessed inappropriately. Please describe (E.g., how often and by whom)
* Custodians, affiliates, volunteers, and contracted personnel will be provided with the clinic’s privacy policies including the privacy charter. Please provide details (E.g., upon hiring and annually)
* Custodians, affiliates, volunteers, and contracted personnel will be required to attend privacy training. Please provide details (how often, type of training)

## Technical Safeguards

The section below provides you with the items that should be covered in your policy and prompts you to provide details on how these safeguards would function in your clinic and the role responsible for the activities. Please review the items and adapt these to describe the safeguards in your clinic.

* The clinic has the following systems in place to protect internal clinic networks carrying identifiable health information from unauthorized use and malicious software. (Please provide details such as firewalls, intrusion detection software, etc.)
* CLINIC NAME information systems users are assigned a unique identifier (User ID) that restricts access to data and application systems to that information based on their functional roles and need to know.
* CLINIC NAME custodians and affiliates only access and use information systems under their assigned User ID. The use of another person’s assigned User ID is prohibited.
* The clinic uses the following methods to control information. Please provide details about how your information systems are controlled. E.g., If a computer is left unattended, how is it protected against unauthorized access? (Manual or automated logout requiring authentication to re-enter the system).
* Passwords are always kept confidential and are not written down, posted publicly, or shared with other staff. Please provide details of how often passwords for the clinic EMR and Alberta Netcare are changed.
* Confidential business or personal information is not sent by email or transmitted over the Internet or external networks without the use of appropriate security measures such as encryption and authentication. Email and fax messages contain a confidentiality notification.
* The clinic systems are monitored to detect unauthorized access and prevent modification or misuse of user data in applications. Appropriate security controls, such as audit logs, are implemented and reviewed as required. Please add details about how this is done in your clinic, for example who does it and how often.
* The computer systems that hold critical or sensitive information are backed up and steps are taken to ensure that backed-up information is stored in a secure environment off-site. Please add details such as how often the computer is backed up, how this is done and what are the steps taken to ensure that backed-up information is stored in a secure environment off-site
* Information intended for long-term storage on electronic media is reviewed (how often?) to ensure the data is retrievable.

# Questions?

If you have any questions about this policy, please contact the clinic’s Privacy Officer,\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.