Health Information

Privacy and Security

Manual

FastMD Family & Walk-in

Prepared: November 2025

Table of Contents

Clinic Profile

Clinic opened:	February 2026
Clinic address:	203-5268 Marlborough Dr NE Calgary, AB T2A, Canada Tel.: 250-528-5743 Email: info@fastmd.ca
Clinic legal structure:	FastMD Family & Walk-in operates under Salma Toma Hanna Professional Corporation.
Type of medical practice:	Family practice
Participating physicians/custodians:	Dr. Salma Toma Hanna
Primary Care Network Membership:	Participates in Mosaic PCN
Clinic Privacy Officer:	Fadi Hanna Clinic Manager

Third party vendor services:

Name	Type of Service	Agreements
Telus Med Access	ASP hosted EMR and IT services – hardware, software, backup service, etc.	IMA
Kyndryl Healthcare IT Services	IT Services – hardware, software, backup services, etc.	Service agreement
Telus	Internet service provider	EULA (service) Contract

Clinic physical description:

Location: FastMD Family & Walk-in is located on the main floor of a strip mall in Calgary, Alberta.

Type of building construction: The building is constructed from a mixture of brick, concrete, and steel.

Clinic location/entrances: FastMD Family & Walk-in has 3 entrances. There are 2 front entrances that open into the waiting area and is used by both staff and patients. The rear entrance is used by staff only. Additionally, FastMD Family & Walk-in has 4 exam rooms, a nurse station, and 3 physician offices.

Measures to protect health information: The clinic has dead bolt locks, security cameras and door alarms. Staff have keys and individually assigned alarm codes.

Fire suppression system: The Clinic has smoke detectors and fire extinguishers.

History of patient records:

2026 to Present: 100% electronic patient records.

Patient records are currently maintained in one clinic database

Backup:
TELUS Med Access:

Backups of clinic data may be maintained outside the provinces of Alberta or BC, but within Canada, and in encrypted format.

Network Files:
Practice backing up (in-house) with an encrypted external hard drive.

Billing Process:
The clinic is currently its own accredited billing submitter. Fee for service codes are indicated by the physicians on a billing sheet. These are entered into the EMR by clinic staff. The submission file is generated by the clinic and transmitted to AH using H-Link.
The clinic intends to continue as the accredited submitter through the ASP Hosted EMR solution.

Electronic lab and DI reporting:
The clinic will continue to receive electronic laboratory and some diagnostic imaging results that will be imported into their EMR database. *(see "Policy Information Flow and Legal Authority" – legal authority for a full description of this process")*. The clinic also receives some paper lab and DI results which are scanned into the EMR.

WCB e-injury reporting:
The clinic will continue to submit its WCB e-injury using a batch channel to enable their accredited third-party software to submit multiple reports to the WCB via a File Transfer Protocol (FTP) process).

Transcription process:

There is no transcription performed at the clinic - physicians enter their own clinic notes and write their own referral / consult letters in the EMR.

Shredding process

Identifying health information is shredded by Clinic staff using a cross-cut shredder. Papers are stored in a locked bin and shredded weekly.

Point of sale:

Point of sale digital receipts are automatically stored within the POS or practice management system (through EMR). Paper receipts, if issued, are filed by date and reconciled daily with the clinic's financial records. Receipts (digital or paper) are typically retained for 7 years.

Information Manager Agreements:

Our clinic has IMA's in place with any and all third-party vendors that have access to any individually identifying patient information. Our Information Manager Agreements (IMA's) comply with section 66 of the *Health Information Act* and 7.2 of the *Health Information Regulation and* are signed by the Custodian.

Privacy Charter

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Introduction

We have adopted this Privacy Charter to guide how our clinic collects, uses, and discloses health information.

Health Information

Our Clinic respects the privacy rights of our patients and is committed to protecting the health information that we collect from you. We have developed our privacy practices based on the *HIA* requirements. This legislation applies to health information we collected, used, and disclosed to provide our patients with health services before and after the *HIA* came into effect. While patient consent can be granted in an informal way, such as providing us with an individual insurance card to document your insurance provider, in some situations we must have formal consent to collect, use, and disclose your personal information.

Principles

Principle 1 - Accountability / Management

We are accountable for the health information you give us.
Our Clinic is accountable for all health information in our possession or control, including any health information that we disclose to other custodians or that we are required to share with third parties to provide you with health services.

We have established policies and procedures aimed at maintaining the privacy of our patients. We have appointed a Privacy Officer to oversee privacy issues for our Clinic. We have educated our employees about our Privacy Policy and their role in protecting your privacy. Patients with questions about our privacy practices are free to contact our Clinic Privacy Officer.

Principle 2 - Notice

We will explain why we collect individually identifying health information before we collect it.
We have posted a notice explaining why we collect your individually identifying health information, and the legal authority that authorizes us to collect it.
We will collect individually identifying health information only for the following purposes, or as otherwise permitted by law:

- *Provision of health services*
- *Verify eligibility or obtain and process payment for health services*
- *Health-Related Educational Communications* (e.g. *a*ppointment reminders, providing information about treatment alternatives, or other health-related benefits and services that may be of interest to you).

Principle 3 - Collection

We limit the amount and type of health information we collect.
Our clinic will only collect health information for the purposes that we have identified or as otherwise permitted by law. In addition, we will only collect as much health information as is essential to carry out the purpose for which we are collecting it.

Your health information will be collected directly from you, except in the limited circumstances where we are authorized by the *HIA* to indirectly collect such information.

Principle 4 - Use and Disclosure

We will use and disclose your health information only for the reasons for which it was provided to us, unless otherwise permitted by law.
In providing health services to you, we may use your health information within the clinic or may disclose it to other custodians to provide you with health services on a basis for the purpose it was collected. Any third-party disclosure of information requires your written consent, unless otherwise permitted by law.

The *HIA* also identifies situations in which the disclosure is mandatory or discretionary. In all cases, we will only disclose as much information as is essential for the purpose it is being disclosed or per *HIA* requirements.

In the future, some of your health information will be deemed "prescribed health information" and we will be required to make it accessible to authorized custodians via the Alberta Electronic Health Record (EHR) [commonly called Alberta Netcare]. Consideration of expressed wishes of the patient will be considered when making your information accessible, and patients can ask for some of their health information to be "masked". When authorized health service providers access health information in Alberta Netcare it is considered a use of health information, not disclosure.

Principle 5 - Consent

We may disclose your health information to a third party with your written consent to that disclosure.
If you consent to disclosure of your health information, you may revoke that consent at any time per the requirements set out in *HIA* (s34). The consequences of withdrawal of consent will be discussed with you and documented.

Principle 6 - Access

You have a right to access your health information that is in our clinic's custody or control within the provisions of HIA.
Patients own the health information in their medical record; the clinic owns the medical record. During the provision of health services, we will share your health information with you or your authorized representative verbally and allow access to or provide copies of your health information records when practical (including information in Alberta Netcare).

As a patient you are entitled to a copy of your medical record, but our clinic also has the right to refuse to disclose health information under some circumstances [*HIA* s11 (1) & (2)] and to make access subject to payment of fees as allowed per *HIA* regulations.

Principle 7 - Safeguards

We will protect your health information from unauthorized access, use, disclosure or destruction.
We have assessed the risks to your health information and implemented administrative, technical, and physical safeguards to eliminate or minimize the risk. Examples of these safeguards include: Clinic policies and procedures that ensure that health information cannot be seen by unauthorized persons, having employees sign oaths of confidentiality to ensure that they understand the importance of confidentiality, electronic security mechanisms like firewalls and password protection, and securing the Clinic when we are closed.

Principle 8 - Quality

We take efforts to ensure that the health information in our custody or control is accurate and complete before using or disclosing that health information.
We update our registration and billing data as required. We ensure that our Clinic records are complete and accurate; we also track additions and amendments. We correct inaccurate or incomplete factual information.

Subject to limited and specific exceptions in the *HIA*, individuals have a right of request corrections or amendments to this information whether in the clinic EMR or Alberta Netcare.

Principle 9 - Retention and Destruction of Records

We will retain your health information per the College of Physicians and Surgeons of Alberta (CPSA) guidelines, and securely destroy of your health information when it is no longer needed.
We will keep your health information per CPSA record retention guidelines or as long as necessary to accomplish the purpose for which it was collected (whichever is longer). We also follow the ten-year retention period per the *HIA* with regard to use and disclosure logs.

We destroy paper health information by shredding and destroy or use professional disk wiping software to remove health information from computer hard drives and other media.

In the event our clinic changes in its provision of health care, patients will be contacted with information about the change and, when applicable, where information has been transferred. You will be free to continue to use that clinic or to have your information transferred to the clinic of your choice.

Principle 10 – Monitoring & Enforcement

We monitor compliance with our privacy policies and procedures and have a process for handling complaints about handling of health information.
We regularly assess our health information safeguards, and ensure our physicians and staff know what they are and that they follow them. We have put in place sanctions for anyone who breaches or attempts to breach our safeguards to demonstrate the important we place on preserving privacy and confidentiality.

We investigate all privacy complaints or suspected privacy breaches, and take appropriate remedial measures including amending our policies, disciplining staff, etc.
We have a process for handling requests for correction or amendments to health information. In the event that a complaint cannot be resolved, the Clinic Privacy Officer will advise the individual of the mechanism for referral of the complaint to the College of Physicians and Surgeons of Alberta, or the Office of the Information and Privacy Commissioner of Alberta.

Personal Employee Non-Health Related Information

Our clinic also respects the privacy rights of **our employees** and is committed to protecting the personal information that we collect from them.

As an employer, we will collect employee's personal information specific to payroll requirements. We will use this information in a way that is reasonable to fulfill our obligations and abide by Personal Information Protection Act (PIPA) legislation in Alberta. The type of information may include:

- letter of employment / contract
- salary or wage history
- performance related documents (including performance reviews, commendations, and disciplinary action)
- tax forms

We will maintain this information securely. Employees have the right to review their own employee records by contacting the clinic Privacy Officer.

Health Information Privacy Clinic

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Purpose

The ***collection***, ***use,*** and ***disclosure*** of ***health information*** by FastMD Family & Walk-in, (hereinafter referred to as the clinic) are governed by the provisions of the *HIA*. The following principles and the procedures appended to this policy are intended to enable patient care and effective service delivery, while protecting the privacy of patients of the clinic.

Scope

This policy applies to:

- physicians and staff, including contractors providing services on behalf of the clinic;
- records in any form created or received in the course of carrying out the clinic's mandated functions and activities;
- all facilities and equipment required to collect, manipulate, transport, transmit, or keep health information.

Clinic

- Clinic staff and contractors shall protect the confidentiality of health information in their custody or control, and the privacy of the individuals who are the subjects of that information. This includes protection against unauthorized use, disclosure, modification, or access to the information.

- Individuals have a right of access to any information about themselves that is in the custody or control of the clinic, in compliance with and subject to the limited and specific exceptions set out in *HIA*. Individuals who believe there is an error or omission in their health information have a right to request to correct or amend the information. All requests will be reviewed by Fadi Hanna, Clinic Privacy Officer (or Attending Physician), before disclosure of records.

- Identifying health information must be collected directly from the individual who is the subject of the information except in the limited circumstances authorized by *HIA* [s22(2)] to indirectly collect such information.

- Every time the Clinic collects individually identifying health information from the individual, the individual must be informed of the purpose for which the information is collected, the legal authority for the collection, and the title, business address, and business telephone number of the Clinic Privacy Officer (or a staff member) who can answer questions about the collection as authorized by *HIA* s22(3)(b). The Clinic provides this information by means of a posted notification sign, "Taking Care of You and Your Health Information" in the reception area.

- Failure to comply with clinic information privacy and security policies and procedures may result in sanctions (including disciplinary action, up to and including termination of employment or contract). Individuals may also be subject to prosecution for the contravention of any law.

Roles and Responsibilities

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Custodians

- Final approval of release/non-release of health information relating to the patients
- Final approval and submission of the Privacy Impact Assessment (PIA) for Clinic-specific health information systems and practices

Clinic Privacy Officer

The *HIA* s62.1 requires custodians to identify a contact person who is responsible for ensuring compliance with the Act. Fadi Hanna is designated as the Responsible Affiliate for the purposes of the *HIA* and given the title of Clinic Privacy Officer.

The responsibilities of the Clinic Privacy Officer include:

Accountability / Management

Ensuring that

- the Clinic health privacy and security policies and procedures are developed and maintained as necessary
- Clinic staff and contractors are aware of their responsibilities and duties under the HIA
- a privacy impact assessment (PIA) is completed and submitted to the Office of the Information and Privacy Commissioner of Alberta (OIPC)
- the Clinic is represented in dealings with third parties and the OIPC of Alberta
- advice on and interpretation of the HIA within the Clinic is provided

Notice

Ensuring that

- the Clinic provides notice about its privacy policies and practices and that the notice identifies the purposes for which health information is collected
- the notice is regularly reviewed and revised as necessary

Consent

Ensuring that

- the Clinic obtains consent with respect to the disclosure of health information where required
- the Clinic has a consent form for the disclosure of individually identifying health information that meets the consent provisions set out in the HIA [s34(2)]

Collection

Ensuring that the Clinic only collects health information for the purposes outlined in the notice as per HIA [s27(1)] or as expressly authorized by an enactment of Alberta of Canada

Use, retention, and disposal

Ensuring that

- the Clinic limits the use of health information to the purposes outlined in the notice as per the HIA [s27(1)] or as expressly authorized by an enactment of Alberta of Canada
- the Clinic retains health information as required by the College of Physicians and Surgeons (CPSA) record retention guidelines, or for as long as necessary to fulfill the stated purpose (whichever is longer)
- all paper copies of health information are disposed of by shredding

Disclosure

Ensuring that health information is only disclosed per the HIA. Any third-party disclosure requires an individual's written consent, unless otherwise permitted by the HIA or another enactment of Alberta or Canada.

Access

- Ensuring individuals have the right of access to information about themselves that is in the custody or control of the Clinic, in compliance with and subject to the limited and specific exceptions set out in the HIA [s7 and 11]
- Responding to requests for access to or correction of health information in the Clinic EMR

Safeguards

Ensuring that

- the overall security and protection of health information in the custody or control of the Clinic per HIA [s60]
- Clinic staff or affiliates sign a Confidentiality Oath and review the Clinic privacy & security policies and procedures at time of hire, annually, upon a change to a job position involving greater health information access or responsibility, or after an incident / breach at the Clinic.
- contractors are given a copy of the Clinic`s privacy & security policies and procedures (on request), as per the vendor non-disclosure agreement (VNDA) or information manager agreement (IMA), and that they sign a declaration that they have received these documents.

Quality

Overseeing reasonable efforts of the Clinic to ensure that the health information in its custody or under its control is accurate and complete, as per the HIA [s61]

Monitoring and enforcement

- Promptly investigating all instances of privacy complaints and breaches using the Clinic 's Privacy Breach Management procedure and taking appropriate remedial measures for substantiated complaints, including where appropriate, amending existing policies and practices or staff disciplinary action
- Ensuring the Clinic PIA is updated periodically to reflect any physical, technical, or administrative changes that may affect the collection, use, or disclosure of health information in the Physician's care or control, as per the HIA. This may require submitting a PIA amendment to the OIPC and should be done within a reasonable time following the changes
- Responding to requests for access to or correction of health information in the Clinic EMR.

All Staff

- Responding to routine requests for access to health information, release of health information, or to correct or amend personal information, where there is no requirement or need to withhold information or deny a request for correction under the HIA
- Identifying privacy breaches and responding in line with the Privacy Breach Management Procedure
- Ensuring the overall security and protection of the health information in the custody or control of the custodians in the Clinic

Right of Access

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Purpose

Subject to limited and specific exceptions in the *HIA*, individuals have a right of access to information about themselves that is in the custody or control of the Clinic and the right to request corrections or amendments to this information. The existence of a current care relationship will be jointly determined by the participating custodian and the individual.

This procedure is intended to define a process for facilitating requests for access to and correction of an individual's health information. Further information about steps to take when dealing with such a request is found in the *HIA Guidelines and Procedures Manual*. The Manual summarizes the rules for collection, use, and disclosure of health information.

Routine Access to Own Health Information

- During the provision of health services, physicians and Clinic staff will share information verbally with the patient or authorized representative and allow access to or provide copies of his / her health information records when practical.
- It is preferable to have a patient request access to his / her own health information by submitting a written request to the Clinic.
- The clinic shall provide access to individually identifying health information only to the individual who is the subject of the information or to his *I* her authorized representative.
- When access to health information is requested by an individual, it will be documented and dated (see Procedure: Disclosure Log).
- A fee may be applied (*HIA* s67) to formal requests for access to their files by patients, or the custodian may choose to waive the fee. The Health Information Regulation sets out the maximum fees that can be charged for providing access.

Formal Request for Access to Information

When patients have not been satisfied with the amount or kind of information that they have received through the clinic's routine procedures, patients may make a **formal request for access** to information in writing. This access request process is detailed in Part 2 of the *HIA*.

- An individual may request access to another person's information only if they are an authorized representative.
- All formal requests for access to information will be processed in accordance with procedures set out in the *HIA* and fees may be charged in accordance with the Health Information Regulation. Any health information or personal information about individual's other than the applicant will be severed before disclosure of the records. Requests will be processed within 30 days of receipt.
- All requests for access to information should be directed to the FastMD Family & Walk-in Clinic Privacy Officer.

- After receiving the request, the Clinic Privacy Officer will retrieve the requested records and, in accordance with the fee schedules set out in the *HIA*, prepare a fee estimate.
- Once the fee estimate is prepared, the Clinic Privacy Officer will notify the applicant of the cost for providing the information requested. The applicant has up to 20 days to indicate if the fee estimate is accepted or to modify the request to change the amount of the fee assessed.
- Processing a request ceases once a notice of estimate has been forwarded to an applicant and begins again immediately on the receipt of an agreement to pay the fee.
- Once the estimate has been agreed to, the Clinic Privacy Officer will review the requested records and, in consultation with appropriate staff prepare the records for disclosure. All records relating to the request will be reviewed on a line-by-line basis to determine possible exceptions to disclosure.
- Access to health information can only be denied based on mandatory or discretionary exceptions outlined in the *HIA* s11. Access requests cannot be denied based on the reason for the request. Any health information or personal information about an individual other than the applicant will be severed before disclosure of the records.
- Where the Clinic Privacy Officer determines that discretionary or mandatory exceptions apply to the records requested, the excepted information will be removed from the record prior to the record being disclosed to the applicant. The applicant will be advised that information has been excepted from disclosure, and under what sections of the *HIA* the exceptions have been made.

Mandatory exception to the right of access

A custodian **must refuse** access to an applicant:

- where the request is for information about a person other than the applicant, unless the information was originally provided by the applicant in the context of a health service being provided to the applicant or the applicant has authority under s104 of the *HIA* to receive the information (e.g., guardian of a minor, executor of an estate for purposes authorized under the Act) [*HIA* s11(2)(a)].
- where the information sets out procedures or contains results of an investigation, a discipline proceeding, a clinic review, or an inspection relating to a health service provider [*HIA* s11(2)(b)].
- where disclosure is prohibited by other law of Alberta [*HIA* s11(2)(d)].

Discretionary exception to right of access

A custodian **may refuse** access to an applicant [*HIA* s11] if the disclosure could reasonably:

- be expected to result in immediate and grave harm to the applicant's mental or physical health or safety
- be expected to threaten the mental or physical health or safety of another individual
- be expected to pose a threat to public safety
- lead to the identification of a person who provided health information to the custodian explicitly or implicitly in confidence and in circumstances in which it was appropriate that the name of the person who provided the information be kept confidential
- be expected to prejudice the use or results of particular audits, diagnostic tests or assessments

Response to the applicant

A response must be made within 30 days of receipt of request unless the time limit has been extended, as allowable by law.

As part of the Clinic's response, the applicant shall be told:

- whether access to the record or partial record is granted or refused
- if access is granted, where, when, and how access will be given

If access is refused:

- The reasons for refusal and basis of refusal and
- The name, title, business address, and phone number of the Clinic's Privacy Officer and that the applicant has a right to request a review of the decision by the Office of the Information and Privacy Commissioner of Alberta

Fee

An initial fee of $25.00 applies to requests under *HIA* s3.2 and will entitle the applicant to up to 20 pages of records [*HIA* s67(3) and Regulation s10(1)]. The attending physician may agree to waive this fee or any other fees for reasons of financial hardship or fairness.

Disclosure log

A file (disclosure log) shall be kept for each request processed (see Procedure: Disclosure Log):

- All internal and external correspondence, including a copy of the original request from the applicant, any notices sent to the applicant, and any other correspondence from the applicant
- An unmarked copy of the records retrieved and reviewed in response to a request
- A copy of the documents released to the applicant
- Any other information documenting the request management process

A Clinic staff member shall be present if the applicant views the original record in order to answer questions and maintain the integrity of the record. If information is severed from the record before disclosure of the information, the applicant no longer has the option of viewing the original record and will view photocopies of the record.

Authentication of recipient

Clinic staff shall take reasonable steps to verify the identity of the individual or authorized representative before allowing access to disclosing health information. This may involve looking at a driver's license or health card.

*A*n authorized representative is any person who can exercise the rights or powers conferred on an individual under applicable privacy legislation (see Appendix I: Definitions) [*HIA* s104(1)]. This includes the right of access to an individual's health information and the power to provide consent for disclosure of such information.

When an authorized representative requests an individual's health information and is not known to the attending physician, proof of authority may be requested. This may involve asking for a copy of such documents as a guardianship order, power of attorney, personal directive, or letters of administration for an estate.

Procedure: Release of Information and Disclosure Log

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Scope

This procedure is intended to facilitate good health records management. A custodian receives four (4) types of release of information requests that are best notated in one disclosure log to provide a common, consistent procedure for the Clinic:

- **Disclosure of a record** containing individually identifying diagnostic, treatment, and care information **without the patient's consent**. This notation is required under the *HIA* and must be maintained for ten (10) years after the disclosure.
- **Disclosure of a record** containing individually identifying diagnostic, treatment, and care information **with the patient's consent**.
- **Routine access requests** from the individual or authorized representation to an individual's own health information. Subject to limited and specific exceptions in the *HIA*, individuals have a right of access to information about themselves that is in the custody or control of the Clinic (Clinic EMR) and the right to request corrections or amendments to this information.
- **Formal access written requests** to an individual's information (when a patient is not satisfied with the information, they received through the Clinic's routine request procedures).
    - *If an individual makes a non-specific formal request to a participating custodian under the HIA s7 for access to their health information, the participating custodian may, at their discretion, access for the purpose of secondary disclosure to the patient*
    - *Further information about steps to take when dealing with a formal access request can be found in the "HIA Guidelines and Procedures Manual". It also summarizes the rules for collection, use, and disclosure of health information.*

This procedure is meant to document FastMD Family & Walk-in's release of information procedures.

Release of information

Our Clinic primarily uses a centralized release of information procedure. Routine requests for information from a patient's record are directed to: Fadi Hanna, the Clinic Privacy Officer.

Any hard copy written report that is disclosed by the Clinic will be labeled "Copy" (or on designated pre-printed paper or other mechanism to identify that this is not an original record). As additional safeguards, a date stamp could be used, and the person responsible for providing the copy (physician, Clinic Manager, etc.) may wish to initial each copied page. In conjunction with the disclosure log, should the copied pages be found by someone other than who they were provided to, the stamp (date and initial) will aid in establishing that the documents were in fact the copies provided and did not originate elsewhere.

Recording expressed wishes of the patient

A patient may specifically request to limit access to their health information in two (2) ways – 1) to limit access within the Clinic to their physician only, or 2) to limit disclosure to any particular recipient (e.g., the patient may request that their most recent diagnosis is NOT made available to their daughter).

In deciding how much health information to disclose, the custodian must consider the patient's expressed wishes, together with any other factors the custodian considers relevant [*HIA* s58(2)].

FastMD Family & Walk-in will record patients expressed wishes not to disclose their health information to particular recipients as a notation in the patient's EMR and/or paper record.

- Each individual who is authorized to disclose information to have access to see can review the notation prior to subsequent disclosure of information.
- Notation
    - Date the patient made the request
    - Which person(s) are not to receive the information
    - Type of information that should not be disclosed
    - Who at the Clinic received the request
    - Author's name (the individual who entered the information).

      For example: Patient has requested that none of his health information be disclosed to his employer, per Dr. ___ (author, date).
- It is important to note that this notation may not be erased when the patient has rescinded the expressed direction. An adjusting entry must be made, including the date of the entry and author's name / details.
  For example: Patient has authorized the disclosure of patient information to the patient's employer, as of _____ (date). See patient consent for same, dated _____

Disclosure <u>without</u> patient consent - continuing care and treatment (may be implied consent) OR disclosure to third party (e.g., Public Health, as required by law)

When health information is released for continuing care and treatment to another care provider (outside of the Clinic) or to anyone other than a custodian without consent (not a care provider and not the patient), the Clinic will inform the recipient in writing of the purpose of the disclosure and authority under which the disclosure is made. The release will be documented in the following manner:

- If transmitted by fax: a copy of the fax cover sheet will be maintained on the paper chart and/or scanned into the EMR, identifying the patient, the individual the information is sent to, the description of the information sent (e.g., Clinic notes from date to date), or a separate entry in the Clinic disclosure log
- If transmitted by mail / courier: 1) a copy of the covering letter will be scanned into the EMR, 2) a notation will be made in the Clinic notes on the date the request was processed, identifying the patient, the individual the information is sent to, the description of the information sent (e.g., Clinic notes from date to date), or 3) a separate entry is made in the Clinic disclosure log

- If transmitted by Secure Electronic mail (email) or eFAX: 1) a copy of the email will be placed into the EMR or paper record, 2) a notation will be made in the Clinic notes, including the date the request was processed, identifying the patient, and the individual the information is sent to, the

description of the information sent (copy and paste email into EMR), or 3) an entry is made in the Clinic disclosure log

Disclosure with patient consent - third party

A file shall be kept for each request processed. The file should include:

- All internal and external correspondence, including a copy of the original request from the applicant, any notices sent to the applicant, and any other correspondence from the applicant
- An unmarked copy of the records retrieved and reviewed in response to a request
- A copy of the documents released to the applicant

The disclosure will be documented in the following manner:

- If transmitted by fax: a copy of the fax cover sheet will be maintained on the paper chart and/or scanned into the EMR, identifying the patient, the individual the information is sent to, the description of the information sent (e.g., Clinic notes from date to date), or a separate entry in the Clinic disclosure log
- If transmitted by mail / courier: 1) a copy of the covering letter will be scanned into the EMR, 2) a notation will be made in the Clinic notes on the date the request was processed, identifying the patient, the individual the information is sent to, the description of the information sent (e.g., Clinic notes from date to date), or 3) a separate entry is made in the Clinic disclosure log

- If transmitted by Secure Electronic mail (email) or eFAX: 1) a copy of the email will be placed into the EMR or paper record, 2) a notation will be made in the Clinic notes, including the date the request was processed, identifying the patient, and the individual the information is sent to, the description of the information sent (copy and paste email into EMR), or 3) an entry is made in the Clinic disclosure log

Release of information to the patient - routine access to own health information

When routine access to health information is requested by an individual, it will be documented and dated as a separate entry in the EMR OR paper patient record.

Release of information to the patient - formal request for access to own health information

A notation will be made in the patient paper record and/or EMR, or a separate entry will be made in the disclosure log.

The notation should include:

- All internal and external correspondence, including a copy of the original request from the applicant, any notices sent to the applicant, and any other correspondence from the applicant
- An unmarked copy of the records retrieved and reviewed in response to a request
- A copy of the documents released to the applicant
- Any other information documenting the request management process

Disclosure Log

Disclosure notations will be kept in the individual patients' electronic and/or paper record. The disclosure log will include the following information:

- The name of the person to whom the custodian discloses the information

- The date and the purpose of the disclosure *(note: not required for databases with electronic logs)*
- A description of the information disclosed
- Patient name
- Patient date of birth
- Patient chart number (if used)
- Date request received
- Records / information requested
- Date of health information Sent
- Prepared by
- Sent to: (name, address)
- Sent by: (mail, fax, email, eFAX, pick up)
- Sent Date
- *(optional)* Fees charged
- *(optional)* Payment received

Procedure: Correction or Amendment of Health Information

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

- When an individual or authorized representative asks for a correction of factual information and can substantiate that the information is incorrect, Clinic staff will make the correction to the Clinic medical record.
  Examples: name, address, telephone number, and other demographic information

- An individual may make a request for correction or amendment in writing to the custodian [*HIA* s13, 14 & 15]. An individual may request a correction to another person's information only if they are an authorized representative (see Appendix 1: Definitions) of that individual.

- The attending physician has **30 days from receipt** of the request to review the records and to **decide whether to grant or refuse the request**. Corrections will only be made to factual information. Corrections cannot be made to professional opinions or observations or to a record that was not originally created by that custodian. Failure to respond within 30 days is deemed as a decision to refuse the request by the custodian.

- **If a correction or amendment is granted**, within 30 days, the custodian must:
  - make the correction or amendment;
  - give written notice to the applicant that the correction or amendment has been made; and
  - notify any person to whom that information has been disclosed during the one-year period prior to the request (unless the custodian believes the applicant will not be harmed by not providing notification to others, and the applicant agrees).

- **If a correction or amendment is refused**, within 30 days, the custodian must give written notice to the applicant that their request is refused and the reasons for that refusal.
  The custodian must also tell the applicant that they can either:
  - ask for a review of the custodian's decision by the Privacy Commissioner; or
  - submit a statement of disagreement within 30 days of not more than 500 words that describes the requested correction or amendment and the applicant's reason for disagreeing with the custodian's decision.
  - If the applicant provides a statement of disagreement, it will be placed on the individual's medical record and copied to any person whom the custodian has disclosed the record to in the previous 12 months.

Policy: Collection, Use, and Disclosure of Health Information

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Principles:

The Clinic will not collect, use, or disclose individually identifying health information if aggregate or other non-identifying health information is adequate for the intended purpose.

When collecting, using, or disclosing health information, the Clinic will only collect, use, or disclose the amount of health information that is essential to enable the Clinic or the recipient of the information to carry out the intended purpose.

Before using or disclosing health information, the Clinic will make a reasonable effort to ensure that the information is accurate and complete.

Collection and use of identifying health information

The Clinic will not use identifying health information to market any service for a commercial purpose or to solicit money without the expressed consent of the individual who is the subject of that information.

Health information will be collected directly from the individual it is about or his/her authorized representative unless indirect collection is authorized by the *HIA*. Examples of indirect collection are:

- When the individual authorizes collection from a third party (this authorization can be verbal)
- When the individual is unable to provide the information, and the custodian collects the information from an authorized representative of the individual
- When direct collection would compromise the interests of the individual, the purpose of the collection, the accuracy of the information, or the safety of another person (e.g., a patient is not completely truthful or cannot remember information)
- When direct collection is not reasonably practicable (e.g., due to a language barrier or cognitive impairment)
- When information is collected from another custodian during referral or consultative processes
- When the information will be used for a purpose authorized under the *HIA* s27, including data matching

When collecting health information directly from an individual, the clinic will inform the individual of the purpose for which the information is collected, the legal authority for the collection and the title and business contact information of a staff member who can answer questions. Notification will be provided by means of a sign or verbally (from the custodian) as appropriate.

The use of individually identifying health information (*HIA s27*) in the custody or control of the custodian(s) can be used for the following purposes:

- Providing health services
- Determining of verifying the eligibility of an individual to receive a health service
- Conducting research or performing data matching or other services to facilitate another person's research (research must be approved by a Research Ethics Board)
- Providing for health services provider education
- Carrying out any purpose authorized by an enactment of Alberta or Canada

- For internal management purposes, including planning, quality improvement, monitoring, audit, evaluation, reporting, or obtaining or processing payment for health services and human resource management.

The use of the clinic's electronic medical record, Alberta Netcare or other electronic applications may be monitored to ensure appropriate confidentiality, and security. Audit and access logs will be checked by the clinic system administrator periodically and/or if a breach of security or privacy is suspected. Alberta Health conducts monthly audits of the information logs of Alberta Netcare. A participating custodian and/or authorized affiliate may access and use information in Alberta Netcare if, and only when:

- They are in a current care relationship with the individual who is the subject of the information;
- They are providing health services to the individual either in the presence or absence of that individual;
- Their access to the information is necessary for the provision of the health services or for making a determination for a related health service; and
- The information is related to and necessary for the current session of care.

Unless alternate use or disclosure is authorized, or required by law, or with the knowledge and consent of the subject individual, individuals have the right to request the Information and Privacy Commissioner to review access, privacy, and correction decisions made by the clinic.

Disclosure of health information

The clinic may disclose individually identifying health information to the individual who is the subject of the information or to his *I* her authorized representative (see APPENDIX 2: DEFINITIONS).

Individually identifying health information may be disclosed to a person other than the subject individual, *if the individual has consented to the disclosure or without consent as allowed per HIA section 35 provisions.*

The clinic requires written consent from the individual to disclose identifying health information to anyone other than the individual or his / her authorized representative, or to another custodian (APPENDIX 3: FORMS). Consent must be provided in writing or electronically and must include:

- the information to be disclosed;
- the purpose for which the information may be disclosed;
- the identification of the person receiving the information;
- an acknowledgement that the person providing the consent is aware of the reasons why the health information is needed, and the risks and benefits of either consenting or refusing to consent;
- the date the consent is effective and expiry date (if any); and
- a statement advising the person that they may revoke the consent at any time.

In deciding how much information to disclose, a custodian must consider as an important factor, any expressed wish of the individual who is the subject of the information relating to disclosure of the information, together with any other factors the custodian considers relevant [*HIA* s58(2)] (Procedure: Release of Information and Disclosure Log).

In all cases, the Clinic will disclose the least amount of identifying health information at the highest level of anonymity that the custodian considers necessary to fulfill the request.

The Clinic may disclose individually identifying health information without the consent of the subject individual. A notation of the disclosure will be made in the chart (a copy of a letter or FAX cover sheet may serve this purpose) (Procedure: Release of Information and Disclosure Log).

- To another custodian or affiliate for the legally authorized uses identified in *HIA* s27
- To a person who is responsible for providing continuing care and treatment to the individual
- To family members of the individual or a close personal friend, if the information is provided in general terms and concerns the presence, location, and condition of the individual on the day on which the information is disclosed
- To contact family members or a close personal friend of the individual, if the individual is injured, ill, or deceased.
- To comply with a subpoena, warrant, or court order.
- If the disclosure is authorized or required by provincial or federal legislation (e.g. *Public Health Act).*
- For the purpose of a court proceeding or proceeding before a quasi-judicial body to which the Clinic is a party
- To the successor custodian of Dr. Salma Toma Hanna or the attending physician.
- To a health professional body for the purpose of an investigation, discipline proceeding, clinic review, or inspection
- To a researcher who has signed a written agreement with Dr. Salma Toma Hanna or the attending physician, in accordance with *HIA* s54, and has provided the Clinic with a copy of the Ethics Board's response to the research proposal

A custodian that discloses a record containing individually identifying diagnostic, treatment, and care information without the patient's consent **must** make a notation of the disclosure [*HIA* s.41(1)]. This notation must be maintained for ten (10) years after the disclosure (Procedure: Release of Information and Disclosure Log).

Disclosure to protect public health and safety

Discretionary disclosure of individually identifying health information to the police or Minister of Justice and Attorney General where a custodian reasonably believes the information relates to the possible commission of an offence under a statute or regulation of Alberta or Canada, and that the disclosure will protect the health and safety of Albertans [*HIA* s37.3(1) and 37.3(2)].

The health information the custodian may disclose is:

- the individual's name
- the individual's date of birth
- the nature of any injury or illness of the individual
- the date on which a health service was sought or received
- the location of where the health service was sought or received
- whether any samples of bodily substances were taken from an individual

Disclosure to Prevent or Limit Fraud or Abuse of Health Services

Discretionary disclosure to the police or to the Minister of Justice and Attorney General under provisions of the *HIA* s37.1 and 37.2 where the custodian reasonably believes the disclosure will prevent or limit fraud or abuse of health services and the disclosure will detect or prevent fraud or limit abuse in the use of health services.

For individuals suspected of fraud or abuse of the health system, the health information that may be disclosed is:

- the individual's name
- the individual's date of birth
- the individual's health number
- the nature of any injury or illness of the individual
- the date on which a health service was sought or received
- the location where the health service was sought or received
- the name and the date of any drug provided or prescribed to the individual

When individually identifying health information is disclosed without the consent of the individual in any of the above circumstances, the name of the person who received the information, the date and purpose of the disclosure, and a description of the information disclosed will be recorded. This record of disclosure must be retained for ten (10) years following the date of disclosure as per *HIA* s41(1).

Additional information is available from the Health Information Act Guidelines and Clinic s Manual, available at:

https://open.alberta.ca/dataset/deb8e064-e4eb-4ad4-a80c-1b932cf6f3e7/resource/483cccd1-915b-47fe-b93b-5aad5e6cead2/download/information-sharing-decision-tree.pdf

Authentication of the Recipient

Clinic staff shall take reasonable steps to ensure the disclosure is made to the person authorized and intended to receive the information. This involves verifying and authenticating the identity of any individual to whom health information is disclosed prior to disclosure.
Examples of proof of identity are:

- photo identification (e.g., a driver's license, passport, etc.)
- a health card
- organization name tag
- business card

Other methods of authenticating include confirming the FAX number provided before sending and confirming that the FAX was received by the intended recipient.

Notation and Notification

When a record containing individually identifying diagnostic, treatment, and care information is disclosed in accordance with *HIA* s35, the Clinic will record the following information in the patient's electronic and/or paper-based health record [*HIA* s41(1)]:

- the name of the person to whom the information is disclosed
- the date and purpose of the disclosure (note: the disclosure purpose is not required for databases with electronic logs)
- a description of the information disclosed

When individually identifying diagnostic, treatment and care information is disclosed to anyone other than the individual themselves or another custodian with or without consent, the Clinic will inform the recipient in writing of the purpose of the disclosure and the authority under which the disclosure is

made. This will be done in the covering letter or FAX cover sheet accompanying the information (APPENDIX 3: FORMS).

Policy: Research

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

The *HIA* contains provisions that expressly govern the disclosure of health information for research purposes. Research is defined as "academic, applied or scientific research that necessitates the use of individually identifying health information" [*HIA* s1(1)(v)].

A person who intends to conduct research using health information in the custody or control of a custodian or health information repository must submit a research proposal to a research ethics board for review. If a board is satisfied with the proposal the researcher may then approach custodians (Clinic s) to ask for disclosure of health information.

Prior to responding to a research request, the Clinic is encouraged to review further information about steps to take when dealing with such a request in the *HIA Guidelines and Clinic s Manua*l section 8.15*)*.

1 A custodian may use individually identifying health information in its custody or under its control for the purpose of conducting research or facilitating another person's research [*HIA* s27(1)(d)]:

1.1. if the custodian or researcher has submitted a proposal to a research ethics board;

1.2. if the research ethics board is satisfied with the research proposal;

1.3. if the custodian or researcher has complied with or undertaken to comply with the conditions, if any, suggested by the research ethics board; and

1.4. if the custodian has obtained consent, when recommended by the research ethics board, from the individuals who are the subjects of the health information (subject individuals) to be used in the research.

2 The following committees and boards are designated as research ethics boards for this purpose:

- Health Research Ethics Board of Alberta;
- University of Alberta - Health Research Ethics Board;
- University of Calgary - Conjoint Health Research Ethics Board

3 If a research ethics board is satisfied with the proposal, the researcher may then provide the following documents to one or more custodians or a health repository:

- their research proposal;
- the board's response to the researcher's proposal; and
- a written application for disclosure of health information to be used in the research, performance of data matching and / or performance of any other service to facilitate research.

4 Upon receipt of the researcher's application and research documents listed in #3, the Clinic Privacy Officer, in consultation with other Clinic custodians, will decide whether to disclose the health information to the researcher or perform services to facilitate the research. The Clinic does **not have** to disclose the information.

5 If the Clinic Privacy Officer decides to disclose the health information or perform data matching or other services to facilitate the research, the custodian **must impose** on the researcher the conditions

suggested the research ethics board and **may impose** other conditions on the researcher. If the board recommended that consents be obtained, the researcher must obtain the consents **before** the disclosure of health information, performance of data matching, or provision of other services.

6 If the Clinic Privacy Officer decides to disclose the health information for research purposes, the researcher must enter into an agreement with the Clinic in which the researcher agrees:

- to comply with:
  - the provisions of the *HIA* and any applicable Regulations;
  - any conditions imposed by Clinic regarding the use, protection, disclosure, return or disposal of the information;
  - any requirements to provide safeguards against the identification of the subject individuals;
- to use the health information only for research purposes;
- to ensure that the information is not published in any form that could lead to the identification of any of the subject individuals involved;
- to only contact subject individuals for additional information, when the Clinic has first obtained the individual's consent to being contacted for that purpose;
- to allow the Clinic to access or inspect the researcher's premises to ensure that the researcher is complying with the terms set out in the agreement; and
- to pay any costs associated with accessing the information *(Note: the Clinic may set the costs, but the cost charged must not exceed the actual cost of providing that service)*.

7 When a research agreement has been entered into by the Clinic, the Clinic may then disclose to the researcher the health information requested, or perform data matching, or other services to facilitate the research. This is to be done with the consent of the subject individuals where recommended by the research ethics board, and without consent where recommended by the research ethics board.

8 If the researcher contravenes or fails to meet the terms and conditions of the agreement with the Clinic, the agreement is cancelled.

Policy: Information Handling

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Purpose

The information security provisions of the *HIA* require custodians to protect individually identifying health information in their custody or control by making reasonable security arrangements to protect against unauthorized access, collection, use, disclosure, or destruction. The Act also requires custodians to take appropriate safeguards for the security and confidentiality of records, including addressing the risks associated with electronic health records. This procedure outlines administrative, technical, and physical safeguards to protect confidential information and electronic health records.

Administrative Safeguards

- The clinic shall ensure that policies and procedures to facilitate the safeguarding of confidential information in its custody or control are developed and maintained. The clinic shall appoint a Clinic Privacy Officer, complete / submit / receive acceptance of a clinic PIA and submit PIA updates for acceptance as required when physical, technical, or administrative changes occur at the clinic that affect the collection, use, or disclosure of health information.
- The need for confidentiality and security of information shall be addressed as part of the conditions of employment for all Clinic staff, beginning with the recruitment stage and included as part of job descriptions and contracts. Clinic staff and affiliates must be aware of and appropriately trained in safeguarding information. A review of Clinic privacy and security policies and procedures must be completed by all Clinic staff and other affiliates at the time of hire, annually, upon a change to a job position involving greater health information access or responsibility, or after an incident / breach at the Clinic. A Confidentiality Oath must be signed at time or hire and annually thereafter. The performance of individuals shall be monitored to reduce the risk of error, fraud, or misuse of information (APPENDIX 3: FORMS). (See Employee Confidentiality and Security Checklist; Netcare pORA requirement).
- Before new users are given access to Netcare, they are provided with system user training, and advised of system confidentiality requirements (i.e. to limit their Netcare access to only pertinent information about a specific patient`s care that they are involved in) and consequences of breaching privacy. Netcare has a large print message on its home page reminding users that the Netcare Portal is monitored and audited on a regular basis and offers users additional training on privacy security and confidentiality through the Alberta Netcare Portal Learning Centre.
- Patients and visitors shall be accompanied by the attending physician or a staff member to examining rooms, offices and non-public areas of the clinic.
- The reception area of the clinic is staffed at all times when the clinic is open, and no-one is allowed behind the reception desk without permission. (Netcare pORA requirement)

- The least amount of information necessary for the intended purpose will be used or disclosed, and only to affiliates or recipients with a ***need to know***. If the intended purpose can be accomplished without use or disclosure of identifying information, then the information should be made anonymous.
- Before implementing new administrative practices or information systems related to the collection, use, and disclosure of health information, the clinic shall complete a privacy impact assessment (PIA) for submission to the Office of the Information and Privacy Commissioner. The PIA will describe how the new initiative will affect privacy, and what measures the clinic will put in place to mitigate risks to privacy.
- Affiliates shall report any violations or breaches of information security as soon as possible to the Clinic Privacy Officer in order that corrective action can be taken to resolve the immediate problem and minimize the risk of future occurrence. The nature of the response will be determined according to the level of gravity of the breach / violation and may include dismissal. Any breach involving Netcare must be reported to Netcare's Information Access and Privacy Office (Manager, Information Policy and Compliance Unit, AB Health and Wellness). *(Netcare pORA Requirement)*
- In order to be granted access to Alberta Netcare a Provincial Organizational Readiness Assessment (pORA) is completed to ensure the clinic's security safeguards meet the minimum requirements needed to be granted access to Netcare. Once a clinic`s application is approved, the clinic must sign an information manager agreement with AH, which outlines the conditions of access and service. The clinic must commit to immediately notify AH of any material change to the clinic`s pORA information. Clinics must also commit to performing a comprehensive TRA at least every two years.
- Our EMR vendor has administrative safeguards in place, including, but not limited to, maintaining and monitoring full audit trails, training vendor and subcontractors on privacy and security awareness, and conducting regular threat risk assessments to ensure risks are identified and mitigated.

Technical Safeguards

- Information system users are assigned a unique identifier (User ID) that restricts access to each data and application systems to that information required for the administration of their duties. Use of user IDs other than that assigned to an individual is prohibited. *(Netcare pORA Requirement)*
- System administrators must have an administrator account for performing system administration. *(Netcare pORA Requirement)*
- Passwords are to be kept confidential at all times and should not be written down, posted publicly, or shared with other staff except for security purposes. Unique passwords or other authentication controls are required for each desktop, network, server, EMR, etc. A strong password standard is used. Passwords for the EMR is changed every 90 days, as prompted by the system. *(Netcare pORA Requirement)*
- All monitors used to display Netcare or other identifying health information will time out after 5 minutes of inactivity and require entry of a password to reactivate the screen. Physicians and staff are to log-off or lock workstations then they leave them unattended to prevent

unauthorized access, especially in patient or public areas of the clinic. All computers are logged off and shut down at the end of the business day. *(Netcare pORA Requirement)*

- Confidential business or identifiable health information will not be sent via e-mail over public or external networks without the use of appropriate security measures such as encryption or by the use of a two-factor authentication connection.
- FastMD Family & Walk-in employees are expected to use the internet responsibly and productively. Internet access is limited to job related activities only and personal use is not permitted.
- Clinic physicians along with administrative staff will have access to billing data.
- The clinic is currently its own accredited billing submitter. Fees for service codes are indicated by the physicians on a billing sheet. These are entered into the EMR by clinic staff. The submission file is generated by the clinic and transmitted to AH using H-Link. The clinic intends to continue as the accredited submitter through the ASP Hosted EMR solution.
- To detect unauthorized access and prevent modification or misuse of user data in applications, use of internal network and Netcare will be monitored by the System Administrator and Netcare to ensure conformity to access policies and standards. Audit and access logs will be checked by the system administrator if a breach of security or privacy is suspected. *(Netcare pORA Requirement)*
- Each user should have a unique user login and password to access the computer network. User rights and accounts will be assigned and maintained by Fadi Hanna. Installation or alteration to system software and hardware will be the responsibility of Fadi Hanna. Fadi Hanna will ensure that original master copies of software are stored with proper physical controls. *(Netcare pORA Requirement).*
- Our Clinic EMR web-based application software, server, data, etc. are hosted offsite by our EMR Vendor. All electronically stored patient data meets the physical, administrative, and technical safeguards outlined in our PIA.
- Our EMR vendor has technical safeguards in place, including, but not limited to, using two-factor authentication for connectivity to the ASP EMR, creating individual system access ID's with strong passwords, daily encrypted backups of EMR data, and the implementation and maintenance of hardware / software firewalls at the ASP facility.
- EMR Client\Server ASP environment where the server environment resides at a TELUS Health Data Center. The connection between the clinic and primary data centre is over a hardware VPN.

  Access from outside of the primary site requires two-factor authentication

  Backups of clinic data may be maintained outside the provinces of Alberta or BC, but within Canada, and in encrypted format.

- The conditions for this service are clearly laid out in our Information Manager Agreement to comply with sections 7.2 and 8(4) of the Health Information Regulation, and section 66(2) of the *Act*. We have confirmed that their location has safeguards that comply with our policies and that the backups will be encrypted and can be restored if required.
- Clinic administrative data (e.g. emails, contact lists, Microsoft documents, etc.) will be backed up daily by the clinic.

- *Network Files:* Practice backing up (in-house) with an encrypted external hard drive.

- The clinic will use an internet service provider to access provincial and regional EHRs. The access will be by a router which acts as a hardware firewall and is regularly patched using approved vendor patches. Each computer in the network has Windows Defender that is updated automatically. The Clinic's EMR vendor has a consistent patch management process in place for its network and workstation operating systems. Patches are applied regularly with critical patches applied as soon as they are released. *(Netcare pORA Requirement)*
- The clinic may request access to Netcare for physicians and key administrative staff. All users will have unique authentication fobs. Alberta Netcare has built the security controls into the system – e.g. use of two factor authentication, encryption of all electronic messages, use of firewalls and intrusion detection systems, logging of all access to the system, and regular auditing. User access is based on role and profession to ensure that users can access the information they need to do their job but, on a need, to know basis.
- Laptops and mobile devices (PDA's, memory sticks, etc.) require layered security protection. Clinic staff using laptops will be provided specific training on mobile computing to ensure that they understand the physical, administrative, and technical safeguards implemented. These include:
  - Ensuring that the Administrator account has been renamed and given a strong password.
  - Never leaving the laptop computer unattended, particularly overnight on desktops. Lock it in a desk drawer or cupboard.
  - Selecting laptop computers that have hard drive (power on) passwords and use these protection measures. Passwords on the hard drive boot sector are more secure than operating system user passwords.
  - Not storing personal or health information on mobile computing devices unless needed.
  - Encrypting individually identifying health information data on the hard drive as well as data on all other mobile devices.
  - Each laptop computer will have a personal firewall installed. Firewalls are not to be turned off by the user; the firewall will be password-protected so that only the network administrator can change it. Users are to request the network administrator to change settings on a firewall when required.
  - Ensuring that the laptop computer's network connection defaults are set to disable automatic roaming.
  - Mobile devices must have, at minimum, unique password settings and, where possible, data encryption enabled.

- **Remote Access to EMR or clinic Computer Network, if applicable**
  - Remote access to the Telus Med Access EMR outside of the Clinic will be granted on a case-by-case / need-to-know basis.
  - Wherever possible, internet connection will be gained using wired network connection.
  - Physician's and authorized Clinic employees and vendors may be granted access to the wireless network and / or remote access to the Clinic computer network.

- Authorized remote access users acknowledge that the Clinic ’s privacy and confidentiality policies and procedures (including wireless networking) and security requirements for the Clinic also apply to the remote access sites (i.e., home offices).

Physical Safeguards

- **Point of sale credit card and debit receipts**: Point of sale digital receipts are automatically stored within the POS or practice management system (through EMR). Paper receipts, if issued, are filed by date and reconciled daily with the clinic’s financial records. Receipts (digital or paper) are typically retained for 7 years.

- **Clinic location/entrances:** FastMD Family & Walk-in is located on the main floor of a strip mall in Calgary, Alberta. FastMD Family & Walk-in has 3 entrances. There are 2 front entrances that open into the waiting area and is used by both staff and patients. The rear entrance is used by staff only. Additionally, FastMD Family & Walk-in has 4 exam rooms, a nurse station, and 3 physician offices.

- **Measures to protect health information:** The clinic has dead bolt locks, security cameras and door alarms. Staff have keys and individually assigned alarm codes.

- Identifying health information will not be displayed or left unattended in public areas. Computer monitors located in the reception area are positioned so that on-screen information cannot be viewed by the general public. *(Netcare pORA Requirement)*

- Identifying health information that is transported between the clinic and other custodians or third parties will be sealed, marked as confidential, and directed to the attention of the authorized recipient.

- Clinic staff will verify the credentials and identity of courier services used to transport health information.

- All fax transmissions will be sent manually with a cover sheet that indicates the information being sent is confidential and giving a telephone number to call if received in error. If preprogrammed numbers are used, a test fax will be sent to each number to verify accuracy before entering that number in the address book. Reasonable steps will be made to confirm that confidential information transmitted via fax is sent to a recipient with a secure fax machine and that fax numbers are confirmed before information is transmitted. A similar confidentiality notice will be affixed to emails sent from the clinic.

- Information that is not confidential or sensitive in nature will be disposed of by placing it in recycling bins and/or shredded in-house.

- Identifying health information is shredded by Clinic staff using a cross-cut shredder. Papers are stored in a locked bin and shredded weekly.

- Before destroying records, it is recommended that a list be made of the names of the patients whose records are to be destroyed, and that this list be kept permanently in a secure location.

The purpose is to be able to later determine at a glance that a medical record has been destroyed and has not simply been lost or misplaced.

- Wireless computer connections are used.

- The below table(s) represents health information stored and accessed by FastMD Family & Walk-in custodians and affiliates. Access is restricted to authorized users during their employment. Accounts are disabled and access to the system is removed when employment terminates.

Practice Data Source	Connection	Access & Storage
TELUS Health Med Access	ASP	EMR Client\Server ASP environment where the server environment resides at a TELUS Health Data Center. The connection between the clinic and primary data centre is over a hardware VPN. Access from outside of the primary site requires two-factor authentication (FOB and password) and a VPN tunnel. Backups of clinic data may be maintained outside the provinces of Alberta or BC, but within Canada, and in encrypted format.
Network files	In-house server	Practice backing up (in-house) with an encrypted external hard drive.
Remote Access		Build on a web-based platform, Med Access is accessed by the physician only from outside of the clinic
Billing Process	H-Link	The clinic is currently its own accredited billing submitted. The fee for service codes is indicated by the physicians on a billing sheet. These are entered into the EMR by clinic staff. The clinic generates the submission file and transmitted to AH using H-Link. The clinic intends to continue as the accredited submitter through the ASP Hosted EMR solution

- Prior to disposal of electronic storage devices (e.g. computers, hard drives, diskettes, tapes, CDs), the media will be destroyed by IT Support under the direction of the privacy officer so as to be unusable.

- Patient health information, in any format (hard copy or electronic), is retained for a minimum of 10 years following the last documented contact with the patient or, in the case of a minor

patient, when the patient reaches 20 years of age (two years past the age of majority) if that is longer than 10 years following the last contact.

- The clinic will maintain documentation for each employee that has received access control items (including identification badges, keys, access cards, fobs, security tokens, perimeter security alarm passwords, computer system passwords, etc.). Key management will include "do not duplicate" engraved on each key provided. When an employee is terminated the clinic will ensure that each item is returned, and / or the access control item is cancelled (passwords cancelled, door locks re-keyed, etc.) *(Netcare pORA Requirement)*

- Transitory records are documents that are required for routine or short-term transactions and contain little or no information of ongoing value. Due to this level of value, these documents should be discarded. This may include temporary information (records required for specific activities but having no further value once the activity has been completed e.g. phone messages, post-it notes).

  Types of transitory records

  - **Temporary information**, such as phone messages, voice mails, post-it notes, invitations and cover sheets.
  - **Duplicates** – exact copies of records maintained as master copies and that have not been altered or added to in any way. Includes photocopies and paper or voice records scanned into or entered into the electronic medical record.
  - **Publications**, including magazines, books, brochures, manuals, etc. that are generally available from other sources.
  - **Direct mail**, including unsolicited mail, brochures, etc. from outside sources.
  - **Blank information media**, including unused forms, diskettes, tapes, etc.
  - **Draft documents**, including source materials used in preparation of documents, draft reports, earlier versions of completed documents. Be sure that draft documents of the following types of records are no longer required for future accountability and documentation purposes:
    - Legal agreements
    - Policies, standards, and guidelines
    - Medical or scientific studies

Policy: Information Security in Contracting

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Contractors who perform a service for FastMD Family & Walk-in have signed an agreement dependent on the level of service provided.

- FastMD Family & Walk-in will ensure IMAs and agreements that identify the requirements outlined under HIA Regulations section 8(4) are in place when engaging with contractors who store data outside of Alberta. This agreement will include specific information security provisions for the contractor or will bind the contractor to the clinic's information security policies and procedures.

- Any related third-party information security and privacy policies should be made available to the Clinic Privacy Officer upon request, including any updates or revisions that occur after execution of the contract.

- All contractors and their employees who have exposure to and use clinic information assets and systems shall sign a confidentiality (non-disclosure) agreement. Third party service providers should remind their employees on termination of their continued responsibility to maintain the confidentiality of the clinic's information. Any privacy breach must be reported to the clinic Privacy Officer within 24 hours.

- Agreements or contracts will include provisions for destroying or returning all clinic information assets, including hardware, system documentation and data upon termination of agreements and in accordance with contract provisions reflecting records retention and data management policy.

Policy: Wireless Networking and Remote Access

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Purpose

To ensure that the risks of transmitting personal and health information are mitigated and that the information is accessible to the clinic for authorized purposes. The intent of these procedures is to include enough technical detail so that the clinic manager can discuss the recovery procedure with the IT professional who will implement.

Clinic policies regarding wireless networking and information handling and security apply at the clinic and anywhere else the authorized clinic devices are used (i.e. home office, telework). These alternate work locations should be discussed with and approved by the system administrator before clinic devices are used.

This policy addresses common security considerations of both wireless and remote access. Our Clinic does plan to implement wireless networking at the Clinic at this time.

Administrative Safeguards

- Complete an inventory of all authorized wireless devices and update the documentation when necessary; annually at minimum
- Document the access point settings in case of reset and have that documentation available both on- and off-site (disaster recovery planning)
- Establish an inventory of wireless devices and other hardware and peripherals connected to the network
- Routinely check for rogue and unauthorized devices (system management)
- The System Administrator will periodically (at least once monthly) monitor any connectivity issues to ensure the integrity of the wireless network
- Review and update all security and access policies, including Wireless Policies, quarterly in recognition that this technology and its inherent risks changes quickly. Provide updates and training to wireless users as required
- Remote access to the EMR outside of the Clinic will be granted on a case-by-case / need-to-know basis

Physical Safeguards

- The router or wireless router and other network equipment, such as a hub, switch, and wireless access point, etc. should be maintained in a restricted location in the Clinic, such as a locked room or secure shelving unit, or attached to a fixed object (e.g., wall).
- UPS (uninterrupted power supply) for router if business continuity and workflow is dependent on wireless connectivity.

Technical Safeguards

Router:

- Firewall has been installed and is active
- Passwords to the router have been changed from the default settings. The administrator password of the router and network should be synchronized.

- Wireless access is password-protected using a minimum 20 characters or greater alphanumeric pass phrase not based on dictionary words
- Scheduled scanning for rogue devices and updates for the wireless network devices is performed; drivers on the wireless devices are periodically updated.
- Disable SNMP (Simple Network Management Protocol)

Wireless access points are secure:

- Use of unique SSID (Service Set Identifier); all computers on the wireless network must have the same SSID as on the wireless access point (AP)
- WPA or WPA2 implemented on the AP and wireless devices
- Change the static IP (Internet Protocol) address on the AP from the default to a different number. Set a static IP address on the wireless clients so that the share the same numbers for the first three octets as the IP address just assigned to the access point, such as 192.168.47.x. Disable the Dynamic Host Configuration Protocol (DHCP) on the AP.
- Turn off administration over wireless (assuming you have at least one computer connected to the wireless access point using a network cable).

Wireless network cards

- MAC address filtering has been turned on and is restricted access to the computer.

Other safeguards

- The System Administrator will lock the authorized client device (laptop) to only connect to pre-defined SSID's and device addresses (and combinations thereof) (which may include designated physician's wireless network in his personal residence).

- Enable the built-in windows firewall on the laptop. Each computer in the network has antivirus protection that is updated automatically (in addition, automatic updates, or ask for, and accept, scheduled updates from Windows and Microsoft office).

- Laptops and mobile devices (PDA's, memory sticks, etc.) require layered security protection. Clinic staff using laptops will be provided specific training on mobile computing to ensure that they understand the physical, administrative, and technical safeguards implemented. These include:
    - Ensure that the Administrator account has been renamed and given a strong password.
    - Never leave your laptop unattended, particularly overnight on desktops. Lock it in a desk drawer or cupboard.
    - Select laptops that have hard drive passwords and use these protection measures. Passwords on the hard drive boot are more secure than operating system user passwords.
    - Do not store personal or health information on mobile computing devices unless you need to. This must be limited to what is necessary, and the data may only be stored for as long as necessary to complete a task. Data must be permanently deleted from laptops once it is no longer required.

    - Data on the hard drive is encrypted as is data on all other mobile devices. Data encryption capability cannot be disabled by the user.
    - Access to physicians EMR's will be provided using the practice owned computers.
- Each laptop will be installed with a personal firewall. Firewalls are not to be turned off by the user; the firewall will be password protected so that only the network administrator can change it. Users are to request the network administrator to change settings on a firewall when required.
- Ensure the laptop's network connection defaults are set to disable automatic roaming.
    - Mobile devices including Blackberry's, iPhones, and memory devices must each have, at minimum, unique password settings and, where possible, data encryption enabled.
- Passwords are to be kept confidential at all times and should not be written down, posted publicly, or shared with other staff except for security purposes. Unique passwords or other authentication controls are required for each desktop, network, server, EMR, etc. A strong password standard is used. Passwords for the EMR are changed every 90 days (minimum) as prompted by the system.
- Wherever possible, internet connection will be gained using wired network connection.
- When using wireless connections outside of the 'trusted zone' (Clinic) is unavoidable, the user will access the internet tools on the web browser to a) delete history, b) clear temporary files, c) clear the cache in virtual memory, d) clear cookies, and e) close the internet browser.
- Physician's and authorized Clinic employees and vendors may be granted access to wireless network and / or remote access to the Clinic local install EMR. Access from outside of the primary site requires two-factor authentication (FOB and password) and a VPN tunnel.
    - Authorized wireless network and / or remote access users acknowledge that the Clinic 's policies and procedures (including wireless networking) and security requirements for the Clinic also apply to the remote access sites (i.e. home offices).
    - When using remote access to the Clinic 's EMR, the user will access the internet tools on the web browser to:
        - delete history,
        - clear temporary files,
        - clear the cache in virtual memory,
        - clear cookies, and
        - close the internet browser.

Wireless Networking Comparison

Wireless Networking Option	Degree of Risk Intercepted / Create Vulnerability	Key Mitigation Strategies
(Best) Wired Network Connection	By far this is the most secure method of gaining internet access	
(Next Best) 802.11 Wireless Networks with WPA2		● WPA2 AES/CCMP encryption on all modern access points and client devices. ● Ensure client devices (each laptop, printers) also have WPA2 enabled ● The pass phrase used to generate the key should be, at minimum, 20 characters long ● The network SSID (name) should not reference the clinic or the location. ● Secure the client devices with software firewalls set to restrict traffic to only the necessary protocols and ports. ● Ensure that the clinic is the only network on the 'preferred network' list (sometimes named other things). Having other network names listed can cause the device to automatically connect to a non-clinic network. ● MAC address filtering (standard on all devices) should be used as an administrative measure only, to ensure that only authorized user devices are allowed on the network despite users knowing the key.
Wi-Fi Based Internet Access	High Risk	● Do not use for sensitive information ● For security reasons, it is best to have clinic laptops stay in the clinic. Taking devices out of the clinic (to home, vacation, conferences, etc.) and wireless hotspots can drastically increase the risk of a device bringing unknown malware into the secure clinic environment and further compromising security. ● Do not use with a device (laptop) that may also access EMR (for example, do not use a laptop to connect to Wi-Fi in the coffee shop and later to the clinic's wired network connection)

Policy: Privacy and Security Risk and Mitigation

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Approach to Risk

Risk can be mitigated through the deployment of controls which will lessen either the likelihood or consequence of a privacy breach. In addition to mitigating risk, an organization can choose to avoid the risk by not undertaking the activity, transfer the risk to another entity or accept the risk. The risk assessment table identifies known risks within a proposed physician office system solution implementation delivered through an WEB-BASED model.

Causes are classified as follows:

1. *People – Internal:* A physician / custodian, an affiliate of the physician/custodian, a person who has legitimate access to the health information held by the Clinic and / or the physician office system, e.g. a transcriptionist, a billing clerk, an allied healthcare provider that works out of the Clinic.
2. *People - External:* A person who is not the physician / custodian, or an Information Manager (IM) affiliate of the physician / custodian, or who does have legitimate access to the health information held by the Clinic and / or the physician office system that has been specifically permitted by agreement or contract. The category includes the EMR vendor or other IT contractors or contact janitors whose access to and authority to use or disclose or alter health information is restricted or circumscribed by Information Manager Agreements or types of confidentiality agreements.
3. *Technology - Internal:* Technology, including electricity supply, cabling, etc. that is under the physical or logical control of the Clinic.
4. *Technology - External:* Technology, including electricity supply, cabling, etc. that is not under the physical or logical control of the Clinic, e.g. is under the control of the EMR vendor or Alberta Health & Wellness.
5. *Physical Security - Internal:* Within the Clinic ’s premises and the immediately adjacent area, there are insufficient physical measures to restrict access to health information in electronic or paper format and / or to restrict access to IT components that if stolen or damaged will result in loss of health information or downtime for the Clinic.
6. *Physical Security - External:* There are insufficient physical measures to restrict access to health information in electronic or paper format, and / or to restrict access to IT components, that if stolen or damaged will result in loss of health information or downtime for the Clinic, that is not under the physical or logical control of the Clinic, e.g. is under the control of the EMR vendor or Alberta Health & Wellness.

The Risk Assessment Table for FastMD Family & Walk-in is: “Attachment - Risk Assessment Table”

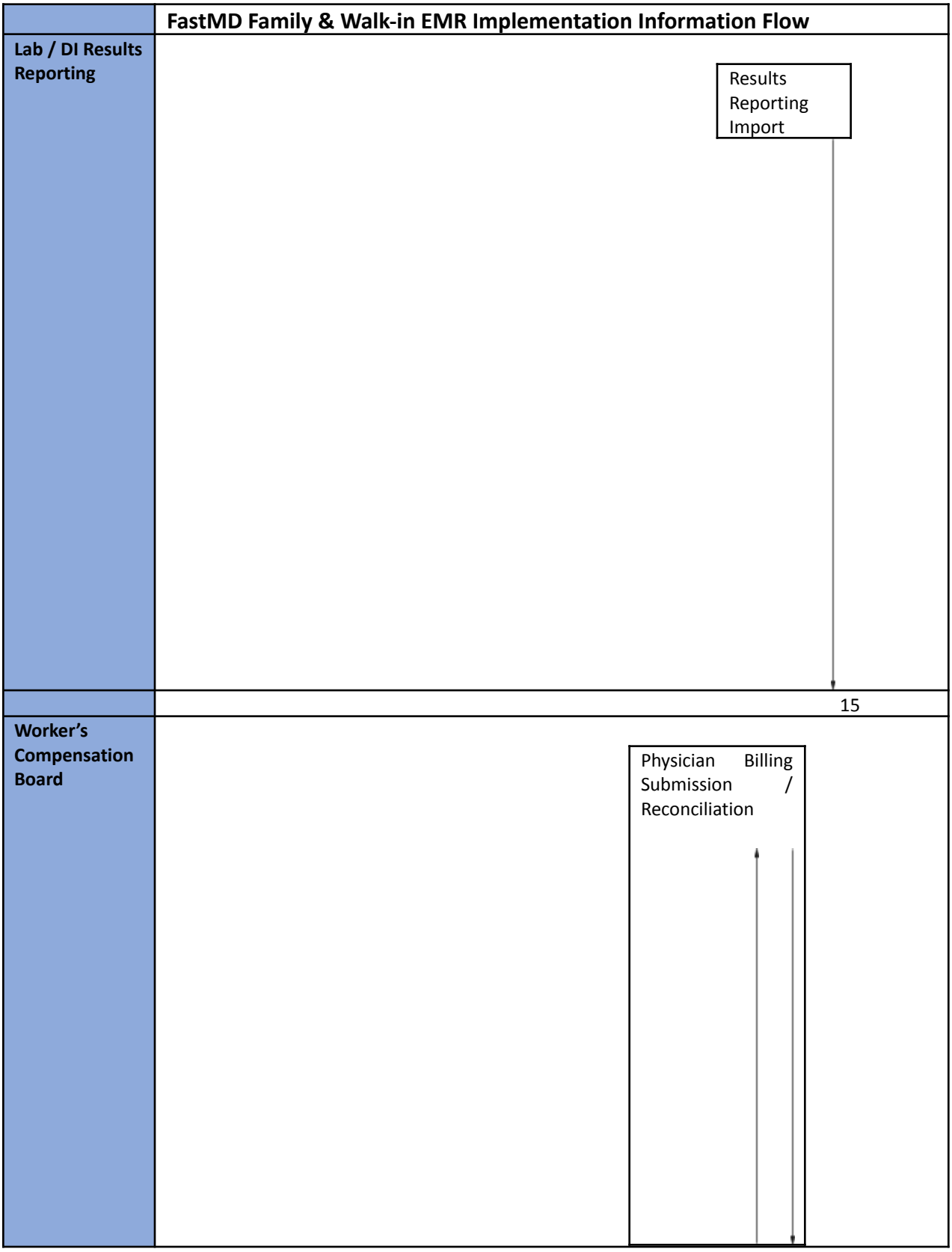
Policy: Information Flow Diagram, Legal Authority Table, and Workflow Diagram

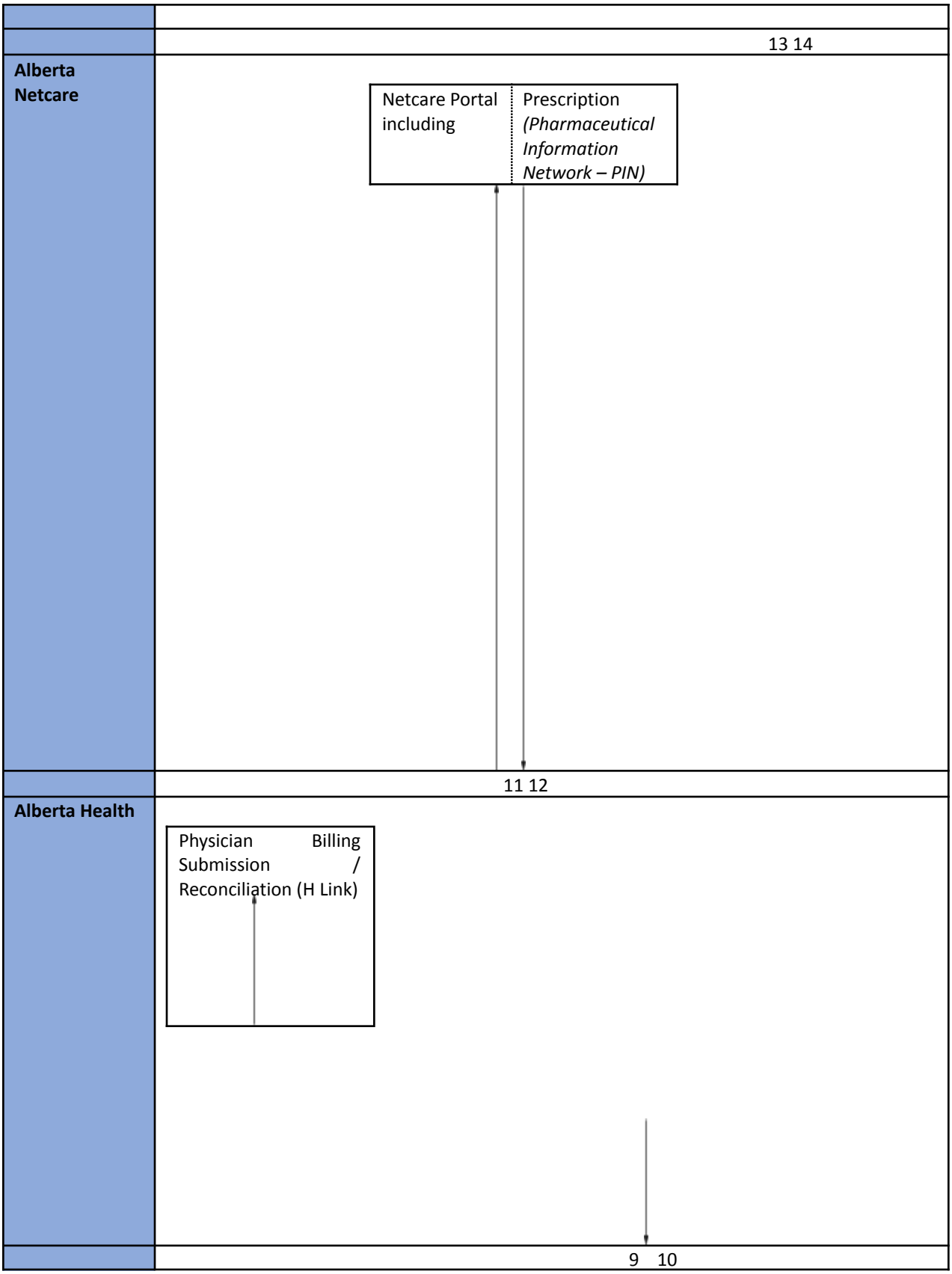
Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

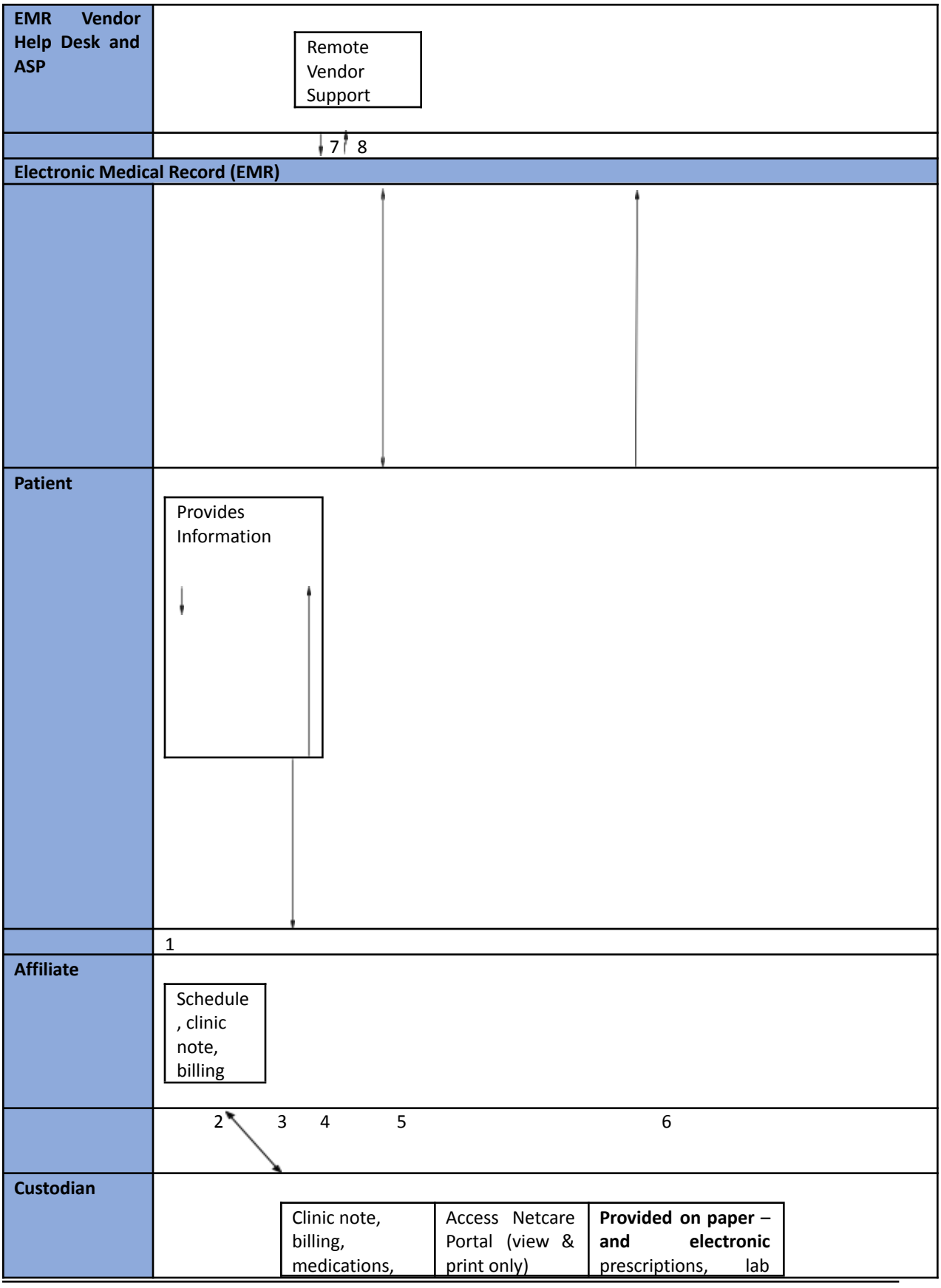
The *HIA* applies to 'health information' in the custody or control of a 'custodian'. *HIA* defines health information as registration information, and diagnostic, treatment and care information. The patient records of FastMD Family & Walk-in contain health information. FastMD Family & Walk-in operates under Salma Toma Hanna Professional Corporation. The physicians working in the Clinic are custodians under *HIA* section 1(1)(f)(ix).

HIA section 66 (2) authorizes a custodian to enter into an agreement with an Information Manager, and section (3) authorizes the provision of health information to an Information Manager without consent of the individuals who are subjects of the information. Section (4) restricts the Information Manager to use or disclose the health information only for the purposes authorized by the IMA. The Clinic has an IMA in place with Telus Med Access.

Information Flow Diagram




13 14
Alberta Netcare
Netcare Portal including
Prescription (Pharmaceutical Information Network – PIN)
11 12
Alberta Health
Physician Billing Submission / Reconciliation (H Link)
9 10


EMR Vendor Help Desk and ASP
Remote Vendor Support
7
8
Electronic Medical Record (EMR)
Patient
Provides Information
1
Affiliate
Schedule , clinic note, billing
2
3
4
5
6
Custodian
Clinic note, billing, medications,
Access Netcare Portal (view & print only)
Provided on paper – and electronic prescriptions, lab

		care, diagnostic, treatment info		requests, DI requests, referrals	

Legal Authority & Purposes Table

Info Flow	Description	Type of Information	Purpose	Legal Authority
1	Patient to Affiliate - schedule, clinic note, billing Collection of health information directly from the patient by affiliate except in set circumstances outlined in *HIA*.	Registration information Diagnostic, treatment and care information	**COLLECTION** Enrolling patient for health service for the purpose of continuing care and treatment, and reimbursement. **USE** Providing health services to the patient	*HIA* sections. 20(a)&(b) 21(1) 22(1)(2) 27(1)(a)(b) & (g)
2	Custodian to Affiliate, Affiliate to Custodian	Registration information Diagnostic, treatment and care information	**USE** **Providing health services to the patient**	HIA sections. 27(1)(a)(b) & (g)
3	Patient to Custodian - clinic note, billing Collection of health information directly from the patient by custodian except in set circumstances outlined in *HIA*. Health information is shared with the patient as part of patient visit – test results, diagnosis, care instructions, etc.	Diagnostic, treatment and care information	**COLLECTION** Purpose of continuing care and treatment, and reimbursement. **USE** Providing health services to the patient	*HIA* sections. 20(a)&(b) 22(1)(2) 27(1)(a)(b) & (g)
4	Custodian (& affiliate as authorized) to patient Informal sharing of patient's health information with patient - consult reports, discharge report, lab results, DI results	Registration information Diagnostic treatment and care information	**ACCESS** Sharing own individually identifying health information with patient	HIA Section 7(1)
5	Custodians, Affiliates to EMR, EMR to Custodians, Affiliates	Registration Information Diagnostic treatment and care information	**COLLECTION** Updates to patient registration for health service for the purpose of continuing care and treatment, and reimbursement. **USE** Providing health services to the patient **DISCLOSURE** Disclosure of diagnostic treatment and care information to the patient	HIA Sections 27(1)(a)(b)(g) 27(2) 56.2 *HIA* s66 (1)(2)(3)(4)(5)(6) (IMA with EMR Vendor;

Info Flow	Description	Type of Information	Purpose	Legal Authority
6	Referrals, prescriptions, lab requests, DI requests (on paper – given to patient or if urgent faxed to other health service provider as allowed under professional guidelines)	Registration information Diagnostic, treatment and care information	**DISCLOSURE to other health service providers** Continuing treatment and care	*HIA* sections 35(1)(a)(b)
7 8	Custodian / Affiliate EMR Help Desk	Registration information Diagnostic treatment and care information	**USE** Technical support and redundancy using privacy principles: least amount; need-to-know; highest anonymity	*HIA* sections 66(1)(2)(3)(4)(5)(6) – IMA in place
9 10	Custodian / Affiliate Alberta Health	Registration information Diagnostic treatment and care information (including health service provider information)	**USE** Processing payment for health services (internal management purposes) Determining or verifying the eligibility of an individual to receive a health service (internal management purposes)	*HIA* section 27(1)(a)(b)(g)
11 12	Access Alberta Netcare Portal to view or print any of the following types of patient information: demographic, prescription (PIN), laboratory data diagnostic imaging text reports, transcribed reports, immunizations (former Capital Health region only), and ECG (former Capital Health region hospitals only)	Registration information Diagnostic treatment and care information	**SHARING AND USE** Providing health services to the patient As of Sept 1, 2011, the list of designated custodians includes the following health services providers – physicians, pharmacists, optometrists, opticians, chiropractors, midwives, podiatrists, dentists, denturists, dental hygienists, and registered nurses.	*HIA* sections 27(1)(a) & 56.2 *HIA* s66 (1)(2)(3)(4)(5)(6) (IMA with AH; can share health information for purposes authorized in the agreement)
13 14	WCB e-injury reporting & claim submission transmitted	Registration information Diagnostic treatment and care information	**Required WCB reporting** **USE** Obtaining or processing payment for health services (internal management purposes)	Worker's Compensation Act *HIA* sections 20(b) 27(1)(a)(b)(g) 35(1)(a)(p)
15	AHS lab and DI test results for patients are received electronically and imported into Clinic EMR; or received on paper / fax, scanned and imported into the Clinic EMR	Registration information Diagnostic treatment and care information	**DISCLOSURE to physician (from other health service providers)** Continuing treatment and care	HIA s35(1)(a)(b) *HIA* s66 (1)(2)(3)(4)(5)(6) (IMA with AHS; can share health information for

Info Flow	Description	Type of Information	Purpose	Legal Authority
				purposes authorized in the agreement)

Procedure: HIA Privacy Breach Management

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Duty to Notify

In 2014, The *Alberta Health Information Act* was amended to include section 60.1 that requires health custodians (or affiliates to custodians) to give notice, in accordance with the regulations, of a loss or any unauthorized access to, or disclosure of individually identifying health information in the custody of control of the custodian if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure. Approved for supporting regulations, the breach reporting requirements took effect on August 31, 2018.

Notification

Section 60.1 of the *Health Information Act* requires notification to the Commissioner, Minister of Health, and affected individual(s) where:

- there has been **any loss of, or any unauthorized access to, or disclosure of** individually identifying health information; and
- there is a risk of harm to the individual who is the subject of the information as a result of the loss or unauthorized access or disclosure.

An access or disclosure is “unauthorized” if it occurs in contravention of the *Health Information Act* or its regulations.

Affiliate’s Duty to Notify

Section 60.1(1) of the *Health Information Act* requires an affiliate of a custodian who becomes aware of any loss of individually identifying health information or any unauthorized access to or disclosure of individually identifying health information in the custody or control of the custodian to, as soon as practicable, notify the custodian in accordance with the regulations.

Custodian’s Duty to Notify

Subsections 60.1(2) and (3) of the *Health Information Act* require a custodian to notify the Commissioner, Minister of Health, and individual who is the subject of the information of any loss of, unauthorized access to, or disclosure of individually identifying health information in the custody or control of the custodian if there is a risk of harm to the individual who is the subject of the information as a result of the loss or unauthorized access or disclosure.

Assessment of Risk of Harm

Where a custodian becomes aware of a loss or unauthorized access or disclosure, the custodian is required to assess whether there is a risk of harm to the individual who is the subject of the information as a result of the loss or unauthorized access or disclosure. If a risk of harm is determined to exist, section 60.1(2) of the *Health Information Act* requires the custodian to undertake notification.

Factors to Consider

Section 8.1(1) of the *Health Information Regulation* sets out the factors that a custodian must consider when assessing the risk of harm. A custodian is required to consider the following factors, in addition to any other relevant factors:

(a) whether there is a reasonable basis to believe that the information has been or may be accessed by or disclosed to a person;
(b) whether there is a reasonable basis to believe that the information has been misused or will be misused;
(c) whether there is a reasonable basis to believe that the information could be used for the purpose of identity theft or to commit fraud;
(d) whether there is a reasonable basis to believe that the information is of a type that could cause embarrassment or physical, mental, or financial harm to or damage the reputation of the individual who is the subject of the information;
(e) whether there is a reasonable basis to believe that the loss of or unauthorized access to or disclosure of the information has adversely affected or will adversely affect the provision of a health service to the individual who is the subject of the information;
(f) in the case of electronic information, whether the custodian can demonstrate that the information was encrypted or otherwise secured in a manner that would
(i) prevent the information from being accessed by a person who is not authorized to access the information, or
(ii) render the information unintelligible by a person who is not authorized to access the information;
(g) in the case of a loss of information, whether the custodian can demonstrate that the information was lost in circumstances in which the information was
(i) destroyed, or
(ii) rendered inaccessible or unintelligible;
(h) in the case of a loss of information that is subsequently recovered by the custodian, whether the custodian can demonstrate that the information was not accessed before it was recovered;
(i) in the case of an unauthorized access to or disclosure of information, whether the custodian is able to demonstrate that the only person who accessed the information or to whom the information was disclosed
(i) is a custodian or an affiliate,
(ii) is subject to confidentiality policies and procedures that meet the requirements of section 60 of the Act,
(iii) accessed the information in a manner that is in accordance with the person's duties as a custodian or affiliate and not for an improper purpose, and
(iv) did not use or disclose the information except in determining that the information was accessed by or disclosed to the person in error and in taking any steps reasonably necessary to address the unauthorized access or disclosure.

The amending Regulation also adds sections 8.2 and 8.3 that detail provisions on the content of the required notice of a custodian to each, the Privacy Commissioner, the Minister of Health, and the affected individual.

Offence

There are several offences related to mandatory breach reporting under the *HIA* (sections 107(1.1) and (1.2)).

It is an offence for a custodian:

- To fail to take reasonable steps in accordance with the *HIA* Regulations to maintain administrative, technical, and physical safeguards that will protect against any reasonably

anticipated threat or hazard to the security or integrity of health information or the loss of health information

- To fail to give notice of a reportable privacy breach under section 60.1(2) of the *HIA* to the Commissioner, the Minister of Health, and affected individuals, in accordance with section 60.1(3) of the *HIA*
- To fail to consider all relevant factors, including the factors prescribed by Regulations, in assessing whether there is a risk of harm to an individual for determining whether notice of a privacy breach must be given, in accordance with section 60.1(4) of the *HIA*
- To fail to give notice to the Commissioner of a decision not to notify an affected individual of a privacy breach in accordance with section 60.1(5) of the *HIA*

It is an offence for an affiliate of a custodian to fail to notify the custodian in accordance with section 60.1(1) of the *HIA* of a privacy breach of individually identifying health information in the custody or control of the custodian.

If guilty of an offence, fines may be applied, as per (section 107(7)) of the *HIA.*

References

Office of the Information and Privacy Commissioner of Alberta – Clinic Note, Reporting a Breach to the Commissioner

Health Information Act Guidelines and Clinic s Manual, Chapter 14 Duty to Notify

Health Information Regulation Amendments: Mandatory Breach Notification, Continuity of Care Leaders Group June 27, 2018

Policy: Password Guidelines

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Purpose:

Ensure that privacy and security of our computer systems are maintained by using a strong password standard.

Policy

Each user will have and use limited privilege accounts for performing job tasks. In particular, each system administrator must each have an administrator account for performing system administration and a limited privilege account for performing non-system administration tasks.

Passwords are to be kept confidential at all times and should not be written down, posted publicly, or shared with other staff except for security purposes. Unique passwords or other authentication controls are required for each desktop, network, server, EMR, etc.

All monitors used to display Netcare or other identifying health information will time out after a short period of inactivity and require entry of a password to reactivate the screen. Selected time-out periods must reflect the level of risk of exposure of workstations.

Each new employee will be given clear directions on how to create a new password for Telus Med Access access and each application. The following are minimum complexity rules requirements for password development.

a minimum length of 8 characters,
no embedded part of name,
a combination of three of the following four: alpha-upper case, alpha-lower case, numeric, special characters,
maximum validity days of 90,
24 iterations required before reuse,
5 maximum invalid attempts before account lockout

The password must contain characters from at least three of the following four categories:

Group	Example
Lowercase letters	a, b, c, ...
Uppercase letters	A, B, C, ...
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Non-alphanumeric (symbols)	( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? /

Policy: Facsimile Transmission Guidelines

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Purpose:

It is to set out guidelines for the clinic to follow to maintain the privacy and security of health information when received and transmitted by fax.

Fax machines, desktop fax software fax modems and fax servers / gateways are common business technologies used to transmit documents. Faxes can be sent from a fax machine to another fax machine or from a computer over telephone lines.

While it is not uncommon for clinics to send health information via fax, there is a risk of inadvertent unauthorized disclosure of information when sending documents via fax. **Unless the health information is required immediately and there is no other practical means of obtaining secure access to the information (e.g. Alberta Netcare look up), custodians should find a less risky mechanism to send the information.** The *HIA* section 60 requires custodians "to protect against reasonably anticipated threat or hazard to the security or integrity of health information or of loss of the health information." Custodians must make a reasonable effort to ensure disclosures are made to the intended and authorized person and are accountability for unauthorized disclosures under *HIA*.

Clinic:

There are situations where the risks to patient care and safety clearly outweighs any potential privacy risk the custodian may face. When faxing is necessary, custodians should follow the following guidelines to reduce the risk of accidental disclosure when **sending** information by fax, including*:

- Limit faxing of health information to
- situations where the information must be faxed;
- Send the most limited amount of information;
- Fax only the personal information which you would feel comfortable discussing over the telephone;
- Always confirm that the recipient has taken appropriate precautions to prevent anyone else from seeing the faxed documents (e.g. their fax is kept in a secure location, or they have someone watching the machine while in operation);
- Any fax machine used to send identifying health information or personal information should be kept in a location where unauthorized persons cannot see the documents. If this is not possible, someone should attend the machine during transmission and reception;
- Consider making one person responsible for sending and receiving documents or send documents yourself. Be prepared to attend the machine to receive documents intended for you if called in advance;
- Use validated, pre-programmed fax numbers where possible (send a test fax to each preprogrammed number to verify accuracy before entering that number in the address book);
- If using auto fax or speed dial, ensure that your directories are up to date on a regular basis;

- Before sending a manual fax, check that the receiver's number is correct, then verify in the machine's display window that you have keyed it in correctly;
- Always complete a clinic fax cover sheet, clearly identifying both sender and intended receiver of the information. The cover sheet should include a confidentiality notice warning that the information is intended for the named recipient only, as well as request the receiver to contact you immediately if the transmission was misdirected.
- When possible, call ahead to ensure that the recipient is there to receive the fax, or call afterwards to ensure he or she received the complete transmission. If neither is possible, check the confirmation sheet to see that it went to the correct number;
- Fax modem (a fax device contained in a computer) – if you are sending information by a fax modem, confirm that other users of the computer system cannot get access to the fax without a password;
- If possible, use encryption technology or other technology to secure fax transmissions;

When faxing is necessary, custodians should follow the following guidelines to reduce the risk of accidental disclosure when **receiving** information by fax, including*:

- Limit your requests to fax health information to you to situations where the information must be faxed;
- Try to arrange a time to receive faxes containing personal information so you can be at the fax machine as they arrive;
- If your fax machine is equipped, use the feature requiring the receiver to enter a password before the machine will print the fax. This ensures that only the intended receiver can retrieve the document. Similarly, ask the sender to make sure you must supply a password to retrieve the document;
- Security precautions should be taken for faxes received after normal office hours;
- Fax modem (a fax device contained in a computer) – If you are expecting information by fax modem, ensure that other users of your system cannot access the information without a password;
- If possible, use encryption technology or other technology to secure fax transmissions;
- Be aware that your fax number can be re-assigned once you have given up the number. It is possible to "purchase" the rights to that line so that the number is never re-assigned.

** Adapted from the Office of the Privacy Commissioner of Alberta's "Guidelines on Facsimile Transmission" (October 2002) and OIPC Investigation Report H2009-IR-004 (May 26, 2009).*

Policy: Email Acceptable Use Guidelines

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

Purpose:

Ensure that privacy and security of our Secure email service are maintained by using an acceptable use standard.
Each user will have unique sign-in (user ID) and password as outlined in Appendix "Password Guidelines" in our HI Policy Manual.
Electronic mail (email) is used in many Health Institutions and Clinical settings and is often the primary communication and awareness method within an organization. At the same time, misuse of email can post many legal, privacy and security risks, thus it's important for users to understand the appropriate use of electronic communications.
The purpose of this email policy is to ensure the proper use of FastMD Family & Walk-in's email system and make users aware of what FastMD Family & Walk-in deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within FastMD Family & Walk-in's Network.
This policy covers appropriate use of any email sent from a FastMD Family & Walk-in's email address and applies to all employees, vendors, and agents operating on behalf of FastMD Family & Walk-in.

Clinic:

All use of email must be consistent with FastMD Family & Walk-in's policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices.

- Any FastMD Family & Walk-in email account should be used for FastMD Family & Walk-in business-related purposes only. No personal communication from these accounts is permitted.
- All FastMD Family & Walk-in data contained within an email message or an attachment must be secured according to the Data Protection Standard.
- Email should be retained only if it qualifies as a FastMD Family & Walk-in business record. Email is a FastMD Family & Walk-in business record if there exists a legitimate and ongoing business reason to preserve the information contained in the email.
- Email that is identified as a FastMD Family & Walk-in business record shall be retained according to FastMD Family & Walk-in's Record Retention Schedule.
- The FastMD Family & Walk-in email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any FastMD Family & Walk-in employee should report the matter to their supervisor immediately.
- Users are prohibited from automatically forwarding FastMD Family & Walk-in email to a third-party email system (non-secure). Individual messages which are forwarded by the user must not contain FastMD Family & Walk-in confidential or above information.
- Users are prohibited from using third-party email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc. to conduct FastMD Family & Walk-in business, to create or memorialize any binding transactions, or to store or retain email on behalf of FastMD Family & Walk-in. Such communications and transactions should be conducted through proper channels using FastMD Family & Walk-in-approved documentation.
- FastMD Family & Walk-in prohibits the use of personal emails, chain letters or joke emails from an FastMD Family & Walk-in email account.

- FastMD Family & Walk-in employees shall have no expectation of privacy in anything they store, send or receive on the Clinic's email system.
- FastMD Family & Walk-in may monitor messages without prior notice.

Compliance:

- Compliance Measurement - The Privacy Officer will verify compliance to this policy through various methods, including but not limited to, periodic walk-through, business tool reports, internal and external audits, and feedback to the Privacy Officer.
- Any exception to the policy must be approved by the Privacy Officer in advance.
- Non-Compliance: An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Attachment: EMR and Data Quality Assurance

Created Date: *November 2025* *Revision Date:*
Applies to: *All Employees and Contractors*
Approved by: *Fadi Hanna*

EMR Data and Functionality Testing

Do not rely on your vendor to test your EMR. You must undertake a comprehensive of your EMR (including billing) especially before and after each version upgrade!! Here are some tips:

1 Create Test Patients in the live database

2 Train using these test patients

3 Reserve some test patients only for testing by authorized users so that you can create specific test scenarios.

4 Capture Screen Prints of how the test patient windows appear. Remember to take screen prints of pop-up dialogue boxes, user preferences, pick lists, audit trails, security settings, user groups, etc.

a. To create screen prints, use 'PRT SCR" button on the keyboard, usually above the Delete key.

b. Paste this image into a word document or use Notepad, Paint, or similar application.

c. Insert instructions, comments, and dates to provide a narrative about the image.

d. Save the new document to your testing files.

e. Print the document and maintain as part of your test scenarios.

5 Create test scenarios that capture the routine day to day functions of your office – for each user type. This also can become your training manual.

f. Remember to include any special enhancements, functionality requests, modifications, or work around that you may have developed or asked your vendor to develop on your behalf. Often these get 'lost' from one version to the next.

6 Print a sample of each report / clinic notes / prescriptions / appointment slips etc that you use in your clinic (using test patients)

Immediately Before the Upgrade:

7 Capture screen prints of the current week using real data for each provider for each date.

8 Print a representative sampling (a select few of real patient records) of each report / clinic notes / prescriptions / appointment slips.

Immediately After the Upgrade and Before Users are Permitted to Enter New 'Real' Data:

9 Re-create steps #7 and #8 and carefully compare your results.

10 Also test each item of functionality that was identified by your vendor as part of the release notes. Use the release notes and your comments as part of the test scenario for next version.

11 Re-create steps in #5 and document your results and comments. Keep as part of the test scenario for next version.

Data Transition Planning

Consider the following EMR Data requirements when changing EMR vendors (now or in the future).

Standard	Vendor Provides	Custodian Provides	Comments
EMR Data			
Orderly transition to the new system that considers data transfer and hardware and software changes?			
If you are transferring data from your old EMR to the new one, how will you ensure data integrity and prevent data loss			
If you run your old system in parallel with your new EMR during a transition period, how will you ensure health information is accurate and complete when it is available from two source systems?			
Do you have a fallback plan in case you discover data integrity or data loss issues in your new EMR?			
What is your quality assurance plan to verify data transfer?			
Once your old system is decommissioned, how will you ensure that data from your old EMR is still available in some form if needed for continuity of care, to respond to access requests under *HIA*, or other legally required disclosures?			
Do you have a plan to securely dispose of data storage media from your old system (and vendor) once it is no longer in use?			
Have you planned staff training on the new system's privacy and security features?			
Record data losses			

These business continuity planning and testing scenarios must be documented and maintained throughout the duration of your medical office and for as long as patient's medical records are maintained. Long after the outgoing EMR and employees are gone, the custodian (physician) may be required to access the patient record *as it was at the time it was created*. This may require a user's knowledge of the EMR system at the time it was in use. These documents and testing scenarios will be valuable to document the collection, use, and access of health information.

APPENDIX 1: ABBREVIATIONS

EMR, Electronic Medical Record
HIA, Health Information Act
IM, Information Manager
IMA, Information Manager Agreement
NDA, Non-Disclosure Agreement
PIA, Privacy Impact Assessment
PMS, Clinic Management System
VNDA, Vendor Non-Disclosure Agreement

23 APPENDIX 2: Definitions

This section provides definitions of the terms used in applicable privacy legislation and Clinic Policies and Procedures.

Affiliate – in relation to a custodian *[HIA section 1(1)(s)]:*

- an individual employed by the custodian;
- a person who performs a service for the custodian as an appointee, volunteer, or student or under a contract or agency relationship with the custodian
- a health services provider who is exercising the right to admit and treat patients at a hospital as defined in the *Hospitals Act*

Affiliate, Information Manager (IM) [*HIA section 66(1)*]

- Information Manager means a person or body that:
    - Processes, stores, retrieves, or disposes of health information,
    - In accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, or
    - Provides information management or information technology services.

Authorized Representative *[HIA section 104(1)]: A*ny person who can exercise the rights or powers conferred on an individual under applicable privacy legislation [*HIA* section 104(1)] (Note: this includes the right of access to an individual's health information and the power to provide consent for disclosure of such information):

- If the individual is under 18 years of age, and does not understand the nature of the right or power and the consequences of exercising the right or power, by the guardian of the individual;
- If the individual is deceased, by the individual's personal representative if the exercise of the right or power relates to the administration of the estate;
- A guardian or trustee appointed under the *Adult Guardianship and Trusteeship Act*, if the right or power relates to the powers or duties of the guardian or trustee;
- An agent under the *Personal Directives Act* if the directive so authorizes;
- A person who has power of attorney granted by the individual if the exercise of the right or power relates to the powers or duties conferred by the power of attorney;
- If the individual is a formal patient as defined in the *Mental Health Act*, by the individuals nearest relative as defined in the *Act* if the exercise of the right or power is necessary to carry out the obligations of the nearest relative under that *Act*; and
- Any person with written authorization from the individual to act on the individual's behalf.

Collect *[HIA section 1(1)(d)]:* To gather, acquire, receive or obtain health information.

Consent *[HIA section 34]:* Agreement by an individual to the disclosure of their own health information to a third party. The consent must include:

- An authorization for the custodian to disclose the health information specified in the consent;
- The purpose for which the health information may be disclosed;
- The identity of the person to whom the health information may be disclosed;
- An acknowledgement that the individual providing the consent has been made aware of the reasons why the health information is needed and the risks and benefits to the individual of consenting or refusing to consent;
- The date the consent is effective and the date, if any, on which the consent expires;

- A statement that the consent may be revoked at any time by the individual providing it - a consent or revocation of consent can be provided in writing or electronically; and
- Electronic consent is valid only if the level of authentication is sufficient to identify the individual who is granting the consent or revoking the consent.

Custodian includes the following [paraphrased from *HIA* section 1(1)(f)]:
- the board of an approved hospital as defined in the *Hospitals Act;*
- the operator of a nursing home;
- an ambulance operator;
- a provincial health board;
- a regional health authority;
- a community health council;
- a subsidiary health corporation;
- a board, council, committee, commission, panel or agency that is created by a custodian;
- a health services provider who is designated in the *HIA* regulations as a custodian: physicians, dentists, pharmacists, registered nurse, optometrists, opticians, chiropractors, midwives, podiatrists, dental hygienists, and denturists.
- a licensed pharmacy;
- the Department;
- the Minister; and
- an individual or board, council, committee, commission, panel, agency, corporation or other entity designated in the regulations as a custodian.

Authorized custodian *[HIA s56(1)(b)]:* a provincial health board, a regional health authority, the Department, the Minister (other than the Health Quality Council of Alberta), and any other custodian that meets the eligibility of the *HIA* regulations [s2(2)] and is a participant in Alberta Netcare.

Data Linking: refers to the merging of files on an identifiable individual for the purpose of ensuring complete registration, diagnostic treatment and care information. For example, unique identifiers are used to populate the EMR with laboratory test results reporting.

Data Matching *[HIA s1(1)(g)]:* means the creation of individually identifying information by combining individually identifying or non-identifying health information or other information from 2 or more electronic databases, **without the consent of the individuals** who are the subject of the information.

Disclosure *[HIA Part 5:* Releasing, transmitting, exposing, revealing, showing, providing copies of, telling the contents of, or giving health information by any means to any person or organization:
- Individually identifying health information shall not be disclosed except in accordance with *HIA*;
- Depending on the situation the *HIA* outlines whether the custodian may, must or must not disclose health information. Most rules in *HIA* say that a custodian ***may*** disclose health information in certain situations;
- Some disclosure situations require consent, and some do not;
- A custodian may disclose non-identifying health information for any purpose (s32.1). If that disclosure of non-identifying information is to a person that is not a custodian, the custodian must inform the person that the person must notify the Commissioner of an intention to use the information for data matching prior to using the information for data matching.

Expressed wishes: A patient may request a custodian to not disclose some or all of their health information to certain people or organizations. The custodian must consider those wishes, and any other relevant factors, when they decide how much health information to disclose.

Health Information: Recorded information about individuals. There are two types of health information:
(1) Registration information (including billing information); and
(2) Diagnostic, treatment and care information.
The collection use and disclosure of both types are regulated by the *HIA*.

Note: Health service provider information is protected differently under the *HIA* effective September 1, 2010. *It is now deemed to be individually identifying information <u>of the individual</u> who received the health service.*

Note: Information collected during provision of pre-employment and insurance physicals for the purpose of determining an individual's fitness to work are not deemed to be health services, nor is the information collected deemed to be health information under *HIA*. Information collected for such services is deemed personal employment information and is protected under PIPA.

Information Manager *[HIA s66(1)]***:** A person or body that:
a) processes, stores, retrieves or disposes of health information;
b) in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information; or
c) provides information management or information technology services.

Effective September 1, 2010, an information manager is now considered an affiliate under HIA.

Record: Health information in any form, including notes, images, audiovisual recordings, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner. This does not include software or any mechanism that produces records.

Research: Academic, applied or scientific research that necessitates the use of individually identifying diagnostic, treatment and care information or individually identifying registration information, or both.

Use: To apply health information for a purpose authorized under *HIA* (s27), and includes the reproduction of information, but does not include disclosing information (e.g. accessing health information within a Clinic to provide patient care or accessing EMR for health information required to provide health services to a patient).

24 APPENDIX 3: FORMS

FORM #1: NOTIFICATION OF COLLECTION OF HEALTH INFORMATION

TAKING CARE OF YOU & YOUR HEALTH INFORMATION

Our Clinic respects your confidentiality and privacy.

When you receive health services from our Clinic, we will collect individually identifying health information in accordance with (s 20) of the Health Information Act (HIA).

We will collect this health information directly from you, except in the limited circumstances where we are authorized under HIA (s 22(2)) to indirectly collect such information.

Our primary purpose in collecting your health information is to:

- Provide diagnostic, treatment and care services to you
- Determine or verify your eligibility for health services
- Bill the Alberta Health Care Insurance Plan for our services

Our Clinic will only collect, use and disclose your health information in accordance with the provisions of HIA.

For more information, please talk to our Clinic Privacy Officer, Fadi Hanna

FastMD Family & Walk-in
203-5268 Marlborough Dr NE
Calgary, AB T2A, Canada
250-528-5743

NOTIFICATION FOR FAX COVER SHEET & EMAIL SIGNATURE BLOCK

This message is intended only for the use of the addressee and may contain information that is privileged and confidential. If you are not the intended recipient, you are hereby notified that any dissemination of this communication is prohibited. If you have received this communication in error, please notify us immediately by phone at 250-528-5743

FORM #2: CONSENT TO THE DISCLOSURE OF INDIVIDUALLY IDENTIFYING HEALTH INFORMATION *[AUTHORIZED BY HIA s34]*

The patient or his/her authorized representative must complete this form before FastMD Family & Walk-in will disclose the patient's health information to someone else (unless Alberta's *Health Information Act* authorizes disclosure without consent).

Patient Information
Patient Name
Date of Birth
What health information do you want disclosed?
Please provide details about the health information you want disclosed, such as the time period of the records
What individual/organization is the patient's health information being disclosed to?
Name of Individua/Organization:
Address, Phone:
What is the purpose for disclosure?
Please provide the reason why you want to disclose the health information (required)
Authorized Representative (required when asking for health information on behalf of another person)
If you are signing on behalf of a patient, please choose one of the options below and provide a copy of supporting documents. I, _____, am ☐ **Guardian** - the parent or legally appointed guardian of the patient who is under 18 years of age and who is not a mature minor in relation to their health information. ☐ **Guardian / Trustee** - the guardian or trustee appointed for the adult patient under the Adult Guardianship and Trusteeship Act exercising my powers or duties as their guardian or trustee ☐ **Agent** - the patient's agent named in an activated Personal Directive under the Personal Directives Act exercising my authority set out in the Personal Directive ☐ **Personal representative** - the personal representative of a deceased patient appointed by the patient's will or by the Court, administering the patient's estate ☐ **Power of attorney** - the patient's named attorney in a Power of Attorney currently in effect exercising my powers and duties conferred by the Power of Attorney ☐ **Nearest relative** - the patient's nearest relative selected in accordance with the Mental Health Act carrying out my obligations as the nearest relative ☐ **Specific decision maker -** the patient's specific decision maker, supportive decision maker, or co-decision maker, authorized in accordance with the Adult Guardianship and Trusteeship Act carrying out the related duties. ☐ **Written authorization** - a person with the patient/client's written authorization to act on the patient/client's behalf
Consent for Disclosure: I authorize FastMD Family & Walk-in to disclose the patient's health information described above to the individual or organization(s) identified above. I understand why I have been asked to disclose my health

information and I am aware of the risks and benefits of consenting or refusing to consent. I understand I may revoke this consent in writing at any time.
Date consent is effective (yyyy-Mon-dd):
Expiry date (yyyy, Mon, dd) (valid for 2 years if not date provided)
Name of person giving consent:
Phone:
Email:
Signature
Date
Information on this form and the supporting documentation are collected under the authorization of sections 20 - 22 of the *Health Information Act* for the purpose of responding to your request and will be filed on the patient record. If you have questions about the collection and use of any information on this form, please contact our privacy officer.

FORM #3: NOTICE TO RECIPIENT to Accompany the Disclosure of Individually Identifying Diagnostic, Treatment and Care Information by a Custodian

DISCLOSURE WITH THE SUBJECT'S CONSENT

(Adapted from *Health Information Act: Guidelines and Clinic s*, Alberta Health 2011)

The attached individually identifying diagnostic, treatment and care information of

_____ is being disclosed to
(name of patient)

_____ by Dr. _____
(name of recipient) *(name of custodian)*

of FastMD Family & Walk-in on _____ with the patient's consent under section 34
(day / month / year)

of the *Health Information Act*, only for the following purpose(s): _____

_____

_____

_____

_____

_____

_____

_____

_____ _____
Name and signature of Custodian (or affiliate) *Date*

(Note: this notice can be used as an individual form added to the fax cover sheet or this information can be added to an existing fax cover sheet)

FORM #4: NOTICE TO RECIPIENT to Accompany the Disclosure of Individually Identifying Diagnostic, Treatment, and Care Information by a Custodian

DISCLOSURE WITHOUT THE SUBJECT'S CONSENT

(Adapted from *Health Information Act: Guidelines and Clinic s*, Alberta Health 2011)

The attached individually identifying diagnostic, treatment, and care information of _____ is being disclosed to _____

(name of subject of information) *(name of recipient)*

by Dr. _____ of FastMD Family & Walk-in

(name of custodian)

- □ To provide continuing treatment and care to the above individual (s.35(1)(b))
- □ To avert or minimize an imminent danger to the health or safety of any person (s.35(1)(m))
- □ To act in the best interests of the above individual if the individual lacks the mental capacity to provide consent (s.35(1)(n))
- □ To provide health services to the above individual who is being detained in a penal or other custodial facility (s.35(1)(e))
- □ To provide information concerning the presence, location, condition, diagnosis, progress and prognosis of the above individual on the above date and the above individual has not requested otherwise (s.35(1)(c)) *(Note – recipient must be a family member or another person with whom the individual is believed to have a close personal relationship)*
- □ To advise family members of the above deceased individual, or a person with whom the above deceased individual is believed to have a close personal relationship, the circumstances surrounding the death of the individual or the health services recently received by the individual and the individual had not requested otherwise (s.35(1)(d.1))
- □ To advise family members of the above individual, or a person with whom the above individual is believed to have a close personal relationship, that the individual has been injured, is ill or has died and the individual has not requested otherwise (s.35(1)d))
- □ To provide necessary health services to a descendant of a deceased individual (s.35(1)(o)) (Note – the recipient must be a descendant or a representative under section 104(1)(c) to (i) and the privacy of the deceased individual must be protected)
- □ To comply with a subpoena, warrant or court order compelling the production of information or with a rule of court that relates to the production of information (s.35(1)(i)) (Note – the recipient body must have jurisdiction to compel the production of information)
- □ To provide information for a court proceeding or a proceeding before a quasi-judicial body (s.35(1)(h) (Note – the custodian must be a party to the proceeding)
- □ To comply with another act or regulation of Alberta or Canada that authorizes or requires the disclosure (s.35(1)(p))
- □ To detect or prevent fraud, limit abuse in the use of health services or prevent the commission of an offence under an enactment of Alberta or Canada (s.35(1)(k)) (Note the recipient must be another custodian)
- □ To provide information to obtain or process payment for health services provided to the above individual by a person that is required under a contract to pay for those services for the above individual (s.35(1)(r))
- □ To provide information to another government (federal/provincial/territorial) when the above individual received a health service in Alberta which is paid for by that government ((s.35(1)(a.1))
- □ To provide information to the College of Physicians and Surgeons of Alberta to administer the Triplicate Prescription Program (s.35(1)(s))
- □ To enable a health professional body to conduct an investigation, a discipline proceeding, a practice review or an inspection (s.35(4)) (Note—the custodian must comply with other relevant legislation and the health professional body must enter into an agreement with the custodian about non-disclosure and destruction of the information)
- □ To transfer records to a successor custodian because the first custodian is ceasing to be a custodian or ceasing to provide health services within the geographic area in which the successor provides health services (s.35(1)(q))
- □ To carry out quality assurance activities within the meaning of section 9 of the Alberta Evidence Act (s.35(1)(g))
- □ To conduct an audit of the information (s.35(1)(f)) (Note – recipient must enter into an agreement with the custodian about non-disclosure and destruction of the information)
- □ To enable an officer of the Legislature (e.g. Auditor General, Ombudsman, Chief Electoral Officer, Information and Privacy Commissioner) to carry out his/her duties (s.35(1)(l))
- □ To enable the Minister of Health and Wellness to carry out his duties (s.40) (Note – the custodian must determine if the disclosure is necessary or desirable)
- □ To allow for permanent preservation and historical research by the Provincial Archives of Alberta or another archives that is subject to this Act or the Freedom of Information and Protection of Privacy Act (s.38) (Note—the custodian must determine that the information has enduring value)

_____ _____

Name and signature of Custodian (or affiliate) *Date*

FORM #5: CONFIDENTIALITY OATH

1 I, _____ agree that I will faithfully discharge my duties as an employee / volunteer / contracted service provider for FastMD Family & Walk-in, and will observe and comply with all policies and procedures of the clinic with respect to privacy, confidentiality, and security of health information.

2 I further acknowledge specific information handling and security practices which include:

a. Information Handling and Security Procedures
b. Laptop Security
c. Wireless Networking / Remote Access Policies

3 Unless legally authorized to do so, I will not use or disclose health or business information (other than business card information) that comes to my knowledge or possession by reason of my affiliation with the clinic, including after I cease to be employed at the clinic.

4 I understand that a breach of this agreement may be just cause for termination of my employment or affiliation with the clinic.

5 I am aware that the clinic has policies and procedures regarding the privacy, confidentiality, and security of health information, and I understand that it is my responsibility to be familiar with the requirements outlined in these policies and procedures. I understand that I am to review these policies and procedures at time of hire, annually, if I change to a job position involving greater health information access or responsibility, or after an incident / breach at the clinic.

6 My use of the clinic's electronic medical record, Alberta Netcare, and other electronic applications may be monitored to ensure appropriate confidentiality, and security. Audit and access logs will be checked by the clinic system administrator periodically and / or if a breach of security or privacy is suspected. Netcare audits user access on a regular basis. A participating custodian and authorized affiliate may access and use information in Alberta Netcare when:

a. They are in a current care relationship with the individual who is the subject of the information;
b. They are providing health services to the individual either in the presence or absence of that individual;
c. Their access to the information is necessary for the provision of the health services or for making a determination for a related health service; and
d. The information is related to and necessary for the current session of care.

7 I understand that I can refer to the Clinic Privacy Officer, Fadi Hanna, for the details of these policies and any other information required for me to understand my obligations.

_____

Signature

_____ _____

Printed Name Date

FORM 6: EMPLOYEE CONFIDENTIALITY AND SECURITY CHECKLIST

Employee Name: _____

Employee Role / Position: _____

Item	Date Completed / Given / Supplied by	Date Returned / Returned to	Comments
Confidentiality Oath *(to be signed at time of hire, annually, upon a change to a job position involving greater health information access or responsibility, or after an incident / breach at the clinic)*			
Review of Clinic Privacy & Security Policies and Procedures (as outlined in the Privacy and Training handbooks), and discussion with Privacy Officer (*to be reviewed at time of hire, annually, upon a change to a job position involving greater health information access or responsibility, or after an incident / breach at the clinic*)			
Main clinic door key			
Other keys (specify)			
Perimeter Security Access Code			
Netcare Access FOB			
Network Computer System User Account			
EMR User Account			

In-Services Attended / Training Attended

Date	Topic	Presented by	Duration
	(Mandatory) Netcare Security Officer or Access Administrator or User training		
	EMR Security Training from EMR Vendor (if hired prior to go live date on EMR)		

Employee Name: _____

Employee Title: _____

Employee Signature: _____

Clinic Representative Name: _____

Clinic Representative Title: _____

Clinic Representative Signature: _____

FORM 7: HIA BREACH REPORTING FORM

Information of Custodian

1. Date of Report:

2. Custodian:

3. Address:

4. Custodian OIPC File #:

5. Contact information for a person who can answer the OIPC's questions about the breach:

Name:

Title/Position:

Mailing address:

Telephone:

Email:

Fax:

Breach Description:

6. Date breach occurred:

7. Date breach ended:

8. Date breach was discovered:

9. Total number of individuals affected (or estimate if not yet known):

10. Was the information collected in Alberta? If yes, the number of individuals whose information was collected in Alberta (or estimate if not yet known):

11. The breach involved a:

Loss of personal information or individually identifying health information.

Unauthorized disclosure of personal information or individually identifying health information.

Unauthorized disclosure of personal information or individually identifying health information.

12. Loss of personal information or individually identifying health information
Location of the breach:

13. Describe the circumstances of the breach and the causes. *Do not include individually identifying information.*

14. Describe how the breach was discovered and who discovered it.

Notice of Affected Individuals

15. Have affected individuals been notified?

16. Describe the content of the notice (***do not include individually identifying information***):

17. Describe the form of the notice (e.g. by letter, email):

18. Date when affected individuals were notified:

19. Copy of notice is attached. ***Do not include individually identifying information*:**

Health Information involved

20. List the types of health information involved. *Do not include individually identifying information.*

Harm

21. Describe the possible harms that may occur as a result of the breach. *Do not include individually identifying information.*

Risk Assessment

22. Provide an assessment of the likelihood that the harm will result. *Do not include individually identifying information.*

Risk Mitigation

23. Describe the steps taken to reduce the risk of harm to affected individuals.

24. Describe the steps taken to reduce the risk of a similar event occurring in the future.

Additional Information

25. Has your privacy officer and/or person responsible for security in your organization been notified of the breach?

If yes, provide the name and contact information of the privacy officer, and the date notified.

Name:
Contact information:
Date notified:

26. Have the police or any other authorities or organizations been notified about the breach?

If yes, provide the name and contact information for each entity notified, and the date notified.

Name:
Contact information:
Date notified:

27. Provide any additional relevant information regarding the privacy breach.

Submitting to the Commissioner

Custodians are required to notify the Commissioner of a reportable breach under the *Health Information Act* **as soon as practicable**.

Email submissions are preferred. Please submit the completed Privacy Breach Report Form to breachreport@oipc.ab.ca.

If you are unable to submit the form by email, you can submit it to:

Office of the Information and Privacy Commissioner of Alberta
410, 9925 - 109 Street
Edmonton, AB T5K 2J8

For general information about responding to a privacy breach, please contact the OIPC by telephone at (780) 422-6860 or toll free 1-888-878-4044.

FORM 8: PASSWORD REQUIREMENTS

Employee Name: _____

Employee Role / Position: _____

Passwords are to be kept confidential at all times and should not be written down, posted publicly, or shared with other staff except for security purposes. Unique passwords or other authentication controls are required for each desktop, network, server, EMR, etc.

All monitors used to display identifying health information will time out after a short period of inactivity and require entry of a password to reactivate the screen. Selected time-out periods must reflect the level of risk of exposure of workstations.

The following are minimum complexity rules requirements for password development.

- a minimum length of 8 characters,
- no embedded part of name,
- a combination of three of the following four: alpha-upper case, alpha-lower case, numeric, special characters,
- maximum validity days of 90,
- 24 iterations required before reuse,
- 5 maximum invalid attempts before account lockout

The password must contain characters from at least three of the following four categories:

Group	Example
Lowercase letters	a, b, c, ...
Uppercase letters	A, B, C, ...
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Non-alphanumeric (symbols)	( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? /

.

List Each Application and Unique Password Requirements:

_____

Signature

_____ _____

Printed Name Date

FORM 9: EMR ACCESS REQUEST

Applicant: _____

Employed by: _____

Job title: _____

Program Area(s): _____

Employee Identifier: _____

Functionality required: (View, create, modify, and print) (registration, Clinic notes, scanning, transcription, and billing)

_____

Remote Access Required? _____ Wireless Access Required? _____

EMR Role Requested: _____

Employee Understanding:

1 I agree that I will faithfully discharge my duties as an affiliate (employee / volunteer / contracted service) provider for FastMD Family & Walk-in and will observe and comply with all policies and procedures of the custodian with respect to privacy, confidentiality, and security of health information.

2 I agree to observe the policies and procedures to ensure privacy, confidentiality, and security of the EMR and the Health Information it contains.

3 I further acknowledge specific Information Handling and Security practices which includes

a. Information Handling and Security procedures
b. Laptop Security
c. Wireless Networking / Remote Access policies
d. Oath of Confidentiality with my employer

Signature: _____ Date: _____

Access Group Recommended: _____ Authorized by: _____

Login Identifier: _____ Created by: _____ _ Date Completed: _____

Date EMR Access Discontinued: _____