Centre de santé communautaire
CHIGAMIK
Community Health Centre

Privacy Policies and Procedures

Protecting your privacy is very important to us. We are committed to informing our clients about CSC Chigamik CHC's Privacy Policy so they know what information we collect, why we collect it, and what we do with it.

CSC Chigamik CHC does not collect, use or disclose any personal and personal health information about clients unless they choose to provide consent to us through a signed consent form. This consent may be withdrawn in full or partially at any time.

CSC Chigamik CHC never collects, uses or discloses information for commercial marketing or any purpose unrelated to our mission and goals, and does not share your information without our clients express consent unless legally required to do so.

Table of Contents

1 INTRODUCTION

1.1 CSC CHIGAMIK CHC is responsible for information it holds regarding clients. Staff at CSC CHIGAMIK CHC must respect and work within organizational policies regarding confidentiality and privacy, consent and release of information. This document contains policies and procedures for CSC Chigamik CHC to govern the sharing of personal health information.

1.2 Following the policies and procedures will help CSC Chigamik CHC to:

1. Comply with their contractual obligations under Data Sharing Agreements (DSA);
2. Comply with their obligations under the *Personal Health Information Protection Act, 2004* (PHIPA);
3. Coordinate their efforts for a common approach to privacy and confidentiality when personal health information (PHI) is shared between healthcare organizations; and
4. Ensure adherence to and compliance with mandates set out by the applicable Health Information Network Providers (HINP) and negate potential breaches through the use of the electronic medical record software, Nightingale on Demand.

2 TERMS AND DEFINITIONS

2.1 The following are a list of terms that you will see throughout these policies and procedures.

Term	Definition
Agent	Agents are persons that, with the authorization of a health information custodian (HIC), for example a hospital, act for or on behalf of the HIC in respect of personal health information for the purposes of the HIC. An agent may or may not be an employee of the HIC and may or may not be remunerated by the HIC.
Common Privacy Framework (CPF)	Common Privacy Framework was developed by Community Care Information Management **(CCIM)** as an overarching framework that establishes a baseline for Privacy practices among community care health service providers **(HSPs)** in Ontario to address the Privacy concerns of HSPs and their clients. In this context, Privacy describes the control clients have over their own personal health information **(PHI)** and how it is collected, used and disclosed by HSPs.
Consent	Consent is clients' permission for a health information custodian (or agent) to collect, use, or disclose personal health information **(PHI).** Consent must be knowledgeable, must relate to the information collected, used or disclosed for a particular purpose, and must be obtained without deception or coercion.
Consent Directive	A consent directive is an express instruction of a client to restrict further use or disclosure of their personal health information.
Data Sharing Agreement (DSA)	A Data Sharing Agreement is an agreement that establishes the mutual terms and conditions related to protecting the privacy and confidentiality of PHI
Electronic Service Provider (ESP)	PHIPA defines an ESP as "A person who provides goods or services for the purpose of enabling a HIC to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information" PHIPA 2004, s. 10 (4).

End-User	End-users are clinical and support personnel with access to the information repository and the PHI contained in it. Clinical users are typically HICs or Agents under PHIPA. Support personnel are typically HINPs or service providers under PHIPA, but may also be Agents.
Health Information Custodian (HIC)	Health information custodians (HICs) are persons or organizations described in PHIPA who have custody or control of personal health information (PHI) as a result of the work they do. Having control of PHI means that a HIC has the right to collect PHI for a variety of reasons (as defined in PHIPA) and they have the obligation to establish information handling procedures that protect privacy and PHI. However the HIC is the owner of the materials and systems in which information is recorded (e.g., paper charts, electronic records, IT systems), each client is the owner of his or her information.
Health Information Network Provider (HINP)	A Health Information Network Providers (HINP) is an organization that provides technology to enable two or more health information custodians to disclose personal health information to one another. The HINP may or may not be an agent of one of the HICs. Like a vendor, a HINP may have physical possession of PHI during service provision, but does not have custody or control of PHI. Each HIC remains fully accountable to their clients for the privacy practices associated with the PHI.
Healthcare Organization	A healthcare organization is used colloquially in these policies and procedures to describe organizations which participate in the shared service described in the Data Sharing Agreement. Although a healthcare organization will usually be a HIC under PHIPA, it may also have other statuses under PHIPA or even no status.
Health Service Providers (HSP)	Includes the following persons and entities:

	1. a person or entity that operates a public hospital under the Public Hospitals Act or a private hospital under the Private Hospitals Act, 2. a person or entity that operates a psychiatric facility under the Mental Health Act, unless the facility is an institution under the Mental Hospitals Act, a correctional institution operated or maintained by Cabinet other than the Minister or a federal prison or penitentiary, 3. an approved corporation that operates and maintains an approved charitable home for the aged under the Charitable Institutions Act, 4. each municipality or a board of management maintaining a home for the aged or a joint home for the aged under the Homes for the Aged and Rest Homes Act, 5. a licensee under the Nursing Homes Act, 6. a community care access corporation within the meaning of the Community Care Access Corporations Act, 2001, 7. a person or entity approved under the Long-Term Care Act, 1994 to provide community services, 8. a not-for-profit corporation that operates a community health centre, 9. a not-for-profit entity that provides community mental health and addiction services, and 10. any other person or entity or class of persons or entities cited in the regulations, and who is also a HIC and a member of the CSC Chigamik CHC
Information And Privacy Commissioner Of Ontario (IPC)	The Information and Privacy Commissioner of Ontario (IPC) acts independently of government to uphold and promote open government and the protection of personal privacy. The IPC is the oversight body for PHIPA. The IPC: 1. Resolves access to information appeals and complaints when government or healthcare practitioners and organizations refuse to grant requests for access or correction;

	2. Investigates complaints with respect to personal information held by government or healthcare practitioners and organizations; 3. Conducts research into access and privacy issues; 4. Comments on proposed government legislation and programs; and Educates the public about Ontario's access and privacy laws.
Information Repository	An information repository is an electronic storehouse of personal health information that may comprise data from multiple points-of-service and be accessible by one or more organizations or facilities.
Log Review	PHIPA requires that access to PHI be on a "need to know" basis, where the need meets PHIPA requirements, not just the job requirements of the person requesting access. To meet this requirement, organizations are required to have controls in place that regulate access and log activities, as well as procedures to regularly review the logs and user access activities. Audit Logs play an important role in this access review process and during breach investigations.
Substitute Decision Maker	If a person is found to be incapable of making sound medical decisions, they will have a substitute decision-maker appointed for them. A substitute decision-maker may be a family member, non-family members are exceptionally rare. The Office of the Public Guardian and Trustee may also be appointed to this role.
Shared Service	Term used within these policies and procedures to describe the information system (whether electronic or manual) that enables two or more HICs to share PHI.
Originating Party	An originating party is a healthcare organization that collects and/or creates personal health information (PHI) and makes it available to other HICs(receiving parties). The original PHI remains under the custodianship of the original party. The

	receiving party has no rights to control the PHI of the originating party.
Personal Health Information (PHI)	Personal health information (PHI) is information about a living or deceased individual. It is information that can identify an individual and that relates to the individual's physical or mental health, the provision of healthcare to the individual, payments or eligibility for healthcare, the donation of a body part or bodily substance, the individual's health number, and the identification of a substitute decision-maker. Examples of PHI: name, medical record number, health insurance number, address, telephone number, PHI related to a client's care (like test results, treatment and medication records, blood type, X-rays and consultation notes) and research-related information (like study participation, test results and sample data).
Personal Health Information Protection Act, 2004 (PHIPA)	The *Personal Health Information Protection Act, 2004* (PHIPA) came into force on November 1, 2004, and governs the collection, use and disclosure of personal health information within the healthcare system in Ontario. PHIPA also has one regulation associated with it, O.Reg. 329/04.
Privacy	In reference to health information, privacy is the right of an individual to control the collection, use and disclosure of his/her personal information; as well as the right to freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.
Privacy Breach	A privacy breach is the unauthorized collection, use, or disclosure of personal health information. This includes the theft or loss of PHI as well as the access or modification of PHI by unauthorized persons. This also includes inappropriate collection, use, or disclosure by authorized individuals.
Privacy Lead	A Privacy Lead is a person designated by each healthcare organization for the purposes of monitoring and ensuring the organization's protection of privacy and PHI related to

	participation in the initiative. This person may be the same as the appointed contact person required by PHIPA (s. 15), a designated employee of a Participating Party to the CSC Chigamik CHC or the Site Contact identified in the DSA.
Receiving Party	A receiving party is a healthcare organization that accesses personal health information (PHI) that was collected, created and made available by other another healthcare organization (originating party) through the shared service. The original PHI remains under the custody and control of the original party. The receiving party has no rights to control the original PHI.
Site Contact	As outlined in the Data Sharing Agreement, the Site Contact is a contact person designated as responsible for the overall administration of the information repository, though this person may designate this responsibility to another party in their organization.
Substitute Decision-Maker (SDM)	A substitute decision-maker is an individual who is identified and authorized to make decisions on behalf of a client, if the client is incapable of making decisions related to the management of their PHI on their own.

3 CONSENT

3.1 PURPOSE

3.1.1 To assist CSC CHIGAMIK CHC and their agents in complying with their statutory obligations under PHIPA in relation to consent and consent directives, and to manage consent and consent directives received from individuals or their substitute decision-makers (SDMs).

3.2 POLICY

3.2.1 OVERVIEW OF CONSENT

Individuals seeking care, or their substitute decision-makers (SDMs) on their behalf, give specific CSC CHIGAMIK CHC custody over their PHI.

Consent of the client is required for the collection, use, and disclosure of PHI except where required by law. Consent will be obtained when information is collected during the initial client intake process. CSC CHIGAMIK CHC will take reasonable steps to ensure that clients understand how and why their information will be collected, accessed, used and disclosed. Staff will only collect information that is necessary to provide service to clients, the community, and to meet legal and funding obligations. All necessary steps will be taken to ensure that information is accurate, complete, and up to date.

Consent can be either implied or express, but in order to be valid the consent must be knowledgeable and for the purposes of this framework, informed.

3.2.1.1 IMPLIED CONSENT

Implied consent refers to situations in which it is reasonable to infer that the client is consenting and it is not necessary to specifically (or expressly) ask for the client's consent. For example, when a client allows their blood to be drawn at a medical laboratory, it is implied that they consent to the results of their blood work to be disclosed to the ordering clinician. Similarly in community care, when a client fills out an intake form that clearly identifies the purposes of the form and what it will be used for and who it will be shared with, then it is reasonable to assume that consent is implied that you will collect this form and use the information in it for the purposes identified without asking specifically "do you consent to this form being used?" Implied consent is only valid if the client is well informed in how their information will be collected, used and disclosed.

3.2.1.2 EXPRESS CONSENT

Express consent refers to situations where consent is given explicitly, either orally or in writing. Express consent does not require any inference on the part of the organization seeking consent. For example, express consent is any situation in which the client is specifically asked "do you consent to the collection, use and disclosure of your personal health information for the purposes of...". Express consent can be verbal or written; and can be signed or checked off on a list. The key to express consent is that the client is specifically asked if they consent.

Consent must be knowledgeable. CSC CHIGAMIK CHC will take reasonable steps to ensure that clients understand how and why their information will be collected, accessed, used, and disclosed.

CSC CHIGAMIK CHC can generally rely on implied consent (assuming the client is knowledgeable) to collect, use and disclose PHI for the purpose of providing healthcare or assisting in providing healthcare.

A healthcare organization must obtain express consent (consent that is explicitly and directly given by the client in oral or written form) when a healthcare organization is:

1. Disclosing PHI to a non-HIC; or
2. Using or disclosing PHI for a reason other than that for which it was collected unless permitted by law.

3.2.2 USE OF PATIENTS HEALTH INFORMATION FOR RESEARCH

PHI in the information repository may not be used for research unless approved by the healthcare organization's Ethics Board (REB) and the research meets all the Research Ethics Board requirements.

Such requests for access to PHI for research purposes must meet all requirements and provision to comply with applicable legislation and development of appropriate tool development, and appropriately trained staff to oversee and audit the project must be weighed against the benefits of the research request.

Where the information repository contains shared records (i.e., records containing PHI that are a sum of contributions from multiple health care providers and which displays or is stored in a format where the record cannot be severed), approval must also be obtained by the Research Ethics Board of the originating parties.

3.2.3 DOCUMENTING CONSENT

Consent should be documented within the client's record to the degree possible and practical. Where documentation within the repository is not possible, consent should be documented elsewhere (particularly for disclosure).

3.2.4 CONSENT DIRECTIVES

3.2.4.1 GENERAL

Clients have the right to establish a consent directive (also known as a lockbox) on their PHI. A consent directive is an express instruction of a client or their SDM to limit or restrict the further use or disclosure of their personal health information.

Consent directives include:

1. The withdrawal of consent to share PHI for healthcare purposes (which results in the client's record being blocked in the information repository); and
2. The reinstatement of consent to share PHI for the purpose of providing or assisting in the provision of healthcare and treatment (which results in the client's record being unblocked).

In order for a consent directive to be implemented, the client must meet with Chigamik's Privacy Office to discuss the specifics of the request and ensure the client understands all of the risk associated with their directive. Following this discussion, the client will fill out either **Appendix F – Consent Withdrawal Form** or **Appendix G – Consent Reinstatement Form** and submit to the Privacy Officer. CSC CHIGAMIK CHC shall honor the consent wishes of a client within 30 days of receiving their completed request form.

Where a client wishes to issue a consent directive, CSC CHIGAMIK CHC shall follow internal policies and procedures for verifying the identity of the client, and where the individual is an SDM:

1. Determining the authority of the SDM to act on behalf of the client; and
2. Documenting the identity of the SDM prior to implementing the consent directive.

CSC CHIGAMIK CHC will receive general directives for consent withdrawal and will follow internal policies and procedures for ensuring that:

1. Clients have provided all required information needed to execute the consent directive; and
2. The client is sufficiently informed about the consequences of consent withdrawal.

CSC CHIGAMIK CHC must be prepared to implement this instruction within the shared service.

3.2.4.2 WITHDRAWING CONSENT

CSC CHIGAMIK CHC will implement withdrawal of consent requests within 30 days of receiving the request in compliance with their internal consent management protocols, ensuring that consent directives are applied within the information repository and/or to the PHI contained in or passing through the information repository to the fullest extent possible.

With paper records, withdrawal of consent shall be managed by placing the client's personal health information in a lock box. Within the information repository, withdrawal of consent shall be managed by engaging functionality whereby access to the client's record is restricted (i.e., "blocked") to healthcare providers with access to the information repository or by preventing the PHI from being sent to the repository. End-users (Health Care Providers) shall be notified that not all information about the client is available via the shared information service using **Appendix H – Notification of Restricted Client Personal Health Information.**

Where, in the course of treatment, a provider is not able to disclose to another provider all the information reasonably necessary for the provision of care, they must notify the recipient. If the withdrawn consent creates a situation where a provider, with or without access, feels the client's safety is at risk, they can refuse to provide treatment when it is not an emergency situation. The provider should explain the reasons for his/her decision not to treat the client and note all relevant discussions in the health record.

3.2.4.3 REINSTATING CONSENT

Reinstatement of consent will result in the relevant records being unblocked within the information repository and being made available to authorized end-users. End-users (Health Care Providers) shall be notified that all information about the client is now available via the shared information service using **Appendix I – Notification of Reinstatement of Consent to Client Personal Health Information.**

CSC CHIGAMIK CHC shall implement reinstatement of consent requests within 30 days of receiving the request, ensuring that consent directives are applied within the information repository and/or to the PHI contained in or passing through the information repository to the fullest extent possible.

3.2.4.4 OVERRIDING CONSENT DIRECTIVES

The shared service shall support sharing overriding consent directives:

- With the express consent of the client or their SDM; or
- Without consent if the healthcare provider deems the blocked PHI as medically significant to the client's well-being and it is not possible to obtain consent in a timely manner

If, during the provision of healthcare or treatment, a healthcare provider requires access to a blocked record:

1. The healthcare provider must either obtain the express consent of the client or their SDM prior to accessing the record, or assert that they are overriding the consent directive without consent because the situation is urgent for the health and well-being of the client;
2. The healthcare provider should indicate within the information repository or through a separate procedure that the healthcare provider has received the client's express consent or the reason for overriding the consent directive without consent; and
3. The shared system will provide the healthcare provider with temporary access to the client's record.

The following information shall be recorded in **Appendix J – Consent Override Notification**:

- Healthcare provider's name
- Date and time of the override
- Whether the override was with or without consent
- If an override with consent:
    - Person who gave consent (i.e., client or SDM). If SDM, their name and relationship to patient
- If an override without consent:
    - Reason for the override without consent

End-users who normally have access to PHI within the information repository do not have the technical capability to override consent directives with the express consent of the client or SDM. CSC Chigamik CHC Privacy Officer is the only user with authority to override a consent directive within the electronic medical system.

All overrides shall be logged and a notice will be sent to the client using **Appendix K – Consent Override Letter**.

3.3 RESPONSIBILITIES

3.3.1 The management of consent and consent directives is a shared responsibility between all healthcare organizations.

3.4 PROCEDURE

3.4.1 OBTAINING CONSENT

To obtain consent, the appropriate agent of the healthcare organization should follow these steps:

1. Ensure the client is providing their knowledgeable consent.
   a. Written public notice should be available and visible in a place where the client is likely to see it;
   b. Staff should be following a consent script when communicating with the client to obtain their consent, particularly if consent is express; and
   c. The notice and script should include:
      i. A general description of the information handling practices (i.e., why PHI is being collected, how it will be used, who has access to it, to whom it will be disclosed);
      ii. A statement indicating that the individual has a right to withdraw or withhold consent;
      iii. How to contact the Privacy Officer (optional for the script);
      iv. How to request access and correct PHI of the client (optional for the script); and
      v. How to make a complaint to the HIC and the IPC/Ontario (optional for the script)
2. Ensure the client understands what they read in the written public notice.
   a. The client should expressly indicate (physically or verbally) that they understand the written notice and that they give their consent (physical or verbal indication) for the collection, use and disclosure of their PHI for the purposes explained to them; and
   b. Staff should answer any questions that may arise, or refer the client to the Privacy Officer.
3. If consent is provided, record the following in the client's record:
   a. Whether the consent was implied or express, who gave consent (i.e., the client or SDM), the date and time that consent was provided, and the person who captured consent via scanning the signed **Appendix A – Service Agreement General Consent to Share Information** and **Privacy Agreement** into the

clients chart. If consent was provided by the client's SDM, the name of the SDM, their relationship to the client, and that their authority to act on behalf of the client has been verified.

4. If the client's PHI is to be shared with another healthcare organization, this is considered a disclosure, and for the disclosure to occur:
   a. Implied consent for the disclosure to another HIC if the client was aware of the planned disclosure at time of collection;
   b. Express consent for the disclosure to a non-HIC or to a HIC if the client was not aware of the disclosure at time of collection; or
   c. The purpose for the disclosure of the client's PHI to another healthcare organization must be aligned with the purposes for which the PHI was originally collected from the client (or their SDM).

3.4.2 WITHDRAWING CONSENT

To administer a withdrawal of consent directive, the Privacy Officer will complete the steps below. The Privacy Officer will explain the possible negative consequences of consent withdrawal to the client or their SDM. In some instances, a clinician may be involved to explain specific clinical impacts that could arise if other healthcare providers are not able to access the client's PHI.

The following process should be followed:

1. The client requests restrictions on use and disclosure of personal health information;
2. Verify the client's or SDM's identity;
3. The Privacy Officer will meet with the client to discuss the request. The Privacy Officer should be clear in explaining that restricting access to their PHI will prevent some or all care providers from being able to access some or all of the client's PHI (as functionality permits). The Privacy Officer should discuss with the client the reasons for requesting consent to be withdrawn, and if appropriate, the potential health risks associated with withdrawing consent;
4. The Privacy Officer will record this discussion and the client's decision in the health record;
5. Explain the limitations or scope of what information may be blocked and to which persons (e.g., entire record to all users or all drug information to all users or to some users);
6. Advise the client that once the withdrawal of consent directive is applied, all blocked care providers will need to obtain express consent to gain temporary

access to the PHI, unless permitted or required by law or where there is a significant risk of bodily harm and consent cannot be obtained in a timely manner;

7. Explain that the client may reinstate consent at any time;
8. Explain that withdrawal of consent is not retro-active and where the information has already been disclosed, it cannot be recalled;
9. Confirm that the client still wishes to proceed with the consent directive;

If the client understands the implications and wishes to withdraw their consent:

- Have the client complete **Appendix F – Consent Withdrawal Form** and submit the form to the Privacy Officer
- Implement the appropriate withdrawal (as functionality permits) where possible; and
- Refer all withdrawal instruction to the HINP where applicable for creating a block within a shared information repository.
- **Appendix H – Notification of Restricted Client Personal Health Information** will be completed by the Privacy Officer and filed in the Clinical Notes section of the health record.
- The Privacy Officer documents in the client's chart that there is locked information.

3.4.3 Overriding a Consent Directive

3.4.3.1 Overriding With Client Consent

To override a consent directive (i.e., for a temporary override of a lockbox) with the client's consent, the Privacy Officer will record the following information in the client's electronic record:

1. Whether consent for the temporary override of the lockbox was given by the client or the client's SDM;
2. The date and time of the override event;
3. The name/initials of the person who collected the consent (If consent was given by the client's SDM, record the name of the SDM).

3.4.3.2 Overriding Without Client Consent

To override a consent directive without the client's consent (e.g., the client is in the Emergency Department and is physically or cognitively unable to provide their consent), the following information will be recorded in the client's electronic record:

1. The date and time of the override event;

2. The name/initials of the person who overrode the consent directive; and
3. The reason for the override (e.g., client unconscious or confused, critical medical emergency)

The shared service should log the user and the date / time of all consent directives overrides. All overrides without client consent shall be logged and a notice will be sent to the client using **Appendix K – Consent Override Letter**. Overrides without consent will be reviewed by CSC Chigamik CHC Privacy Officer to ensure the override without consent was appropriate.

3.4.4 REINSTATING CONSENT

If a client wishes to reinstate their consent to share their PHI, the appropriate agent of the healthcare organization will:

1. Verify the client's identity;
2. Explain that a reinstatement of consent will remove the client's information block on their records and permit all other providers who care for the client and use the information repository to access his or her records for the purpose of providing or assisting in the provision of healthcare services to the client;
3. Explain that once the block has been removed, authorized healthcare providers will not have to obtain express consent from the client to access their record of PHI;
4. Explain that the client may again withdraw their consent at any time;
5. Based on the functionality that exists, a client may be able to remove the mask from some or all of their PHI enabling access to some or all authorized users;
6. Implement the appropriate reinstatement (as functionality permits) where possible, and refer all reinstatement instruction to the HINP where needed for removing a block within a shared information repository; and
7. Notify the end users using **Appendix I – Notification of Reinstatement of Consent.**

3.4.5 PAPER CHARTS – USING A LOCK BOX

The lock box is located in a Lock Box file in the secure healthcare record room.

The process outlined below will be followed when implementing a lockbox on paper records:

1. The client requests restrictions on use and disclosure of personal health information;
2. Verify the client's or SDM's identity;
3. The Privacy Officer will meet with the client to discuss the request. The Privacy Officer should be clear in explaining that restricting access to their PHI will prevent some or all care providers from being able to access some or all of the client's PHI (as functionality permits). The Privacy Officer should discuss with the client the reasons for requesting consent to be withdrawn, and if appropriate, the potential health risks associated with withdrawing consent;
4. The Privacy Officer will record this discussion and the client's decision in the health record;
5. Explain the limitations or scope of what information may be blocked and to which persons (e.g., entire record to all users or all drug information to all users or to some users);
6. Advise the client that once the withdrawal of consent directive is applied, all blocked care providers will need to obtain express consent to gain temporary access to the PHI, unless permitted or required by law or where there is a significant risk of bodily harm and consent cannot be obtained in a timely manner;
7. Explain that the client may reinstate consent at any time;
8. Explain that withdrawal of consent is not retro-active and where the information has already been disclosed, it cannot be recalled;
9. Confirm that the client still wishes to proceed with the consent directive;

If the client understands the implications and wishes to withdraw their consent:

- **Appendix F – Consent Withdrawal Form** will be filled out and the original will be stored in the clients chart;
- If the restricted information is already in the health record, a copy is made, the original section in the notes is 'blacked out' and the copy put into a sealed envelope;
- If the original information has not been written in the health record, then it can be written on a separate note and put into the sealed envelope for the lock box;
- The restricted information is put into a sealed envelope with the completed **Appendix F –Consent Withdrawal Form**. The client's identifying data is put on the outside of the envelope which is placed into the Lock Box.
- **Appendix H – Notification of Restricted Client Personal Health Information** will be completed by the Privacy Officer and filed in the Clinical Notes section of the health record.

- The Privacy Officer documents in the client's chart that there is locked information.

4 INDIVIDUAL ACCESS & CORRECTION

4.1 PURPOSE

4.1.1 To fill permitted requests for access or correction to PHI from individuals (or their SDMs) whose information is collected, used or disclosed via the information repository.

4.2 POLICY

4.2.1 GENERAL

Individuals may request access to and correction of their PHI retained in the custody or control of a HIC. Clients have the right to:

- Access their information for their review;
- Request a correction of information;
- Have assistance in interpreting their record; and
- Obtain a copy of their record

The individual requesting access to their PHI must fill out **Appendix M – Request for Access of Client Records** and provide the completed form to the Privacy Officer.

4.2.2 RESPONDING TO ACCESS REQUESTS

CSC Chigamik CHC must respond within 30 days of receiving the request, or may extend the deadline upon by providing written notification to the requestor. If the reason for the delay is related to the information repository technology, the healthcare organization will notify the HINP Site Contact and Privacy Officer immediately, who will work with information technology staff to resolve the delay.

If the information requested was not collected, created, sent, received, or otherwise used or relied upon for the provision of healthcare by the healthcare organization receiving the request, the request should be directed to the party(ies) that collected the information initially.

Assistance in understanding the record will be the responsibility of the primary care provider. Should the provider believe that releasing information could be harmful to the client the provide may suggest having an appointment to review the information requested.

4.2.3 RESPONDING TO CORRECTION REQUESTS

Only the healthcare organization that initially collected the client's PHI can respond to the correction request. This is because only the care provider that originally collected

the PHI can comment on the accuracy of the PHI and the appropriateness of the correction request.

Where a correction request is the result of an access request (i.e., receiving a report containing all clinical information retained in the information repository), the client must request a correction in writing to the originating party. If the original party is CSC Chigamik CHC, the client must fill out **Appendix N – Request for Correction of Client Records** and provide the form to the Privacy Officer. The Privacy Officer will then work with the health care provider to ensure the accuracy of data in the chart.

Healthcare organizations that receive correction requests for a record that was created by or received from another organization should inform the client to contact the originating party.

CSC Chigamik CHC will review, process, respond and track all correction requests in accordance with internal policies and procedures.

4.3 CHARGING ACCESS FEES

CSC CHIGAMIK CHC may charge individuals for copies of their records in compliance with their procedures governing access. The fee are nominal, to offset the administrative costs associated with providing access to the record.

Where there is a shared repository and where the HINP has the capacity and permission (from the healthcare organizations) to fill access requests, healthcare organizations will agree to a harmonized fee schedule.

See fee structure chart in Section 5.3.2 Charging Access Fees, for more details.

4.4 RESPONSIBILITIES

Each healthcare organization is responsible for responding to access and correction requests pertaining to the PHI which it initially collected. If the PHI being requested includes information that was originally collected by another provider, the Privacy Officer at the organization to which the request was made shall work with the Privacy Officer at the other organizations to provide the client with access to all or some of his or their PHI.

Corrections to PHI as the result of a system-generated error will be reviewed by the healthcare organization that originally collected the PHI and be completed by the HINP as required. Where information is modified as the result of a correction, the original information must be retained to ensure legislative, legal and professional requirements are met for record keeping.

Please refer to the chart below for a breakdown of the appropriate procedure.

Requested Information		Affected Healthcare Organization(s)	Action
PHI that the healthcare organization never collected, used or disclosed for care		Healthcare organization with the potential to access PHI for which they do not have custody, are not the originating party, and which they have not accessed, used or disclosed for the purpose of providing healthcare	1. Do not provide access to the PHI. 2. Refer the client to the appropriate parties involved.
PHI the healthcare organization collected, created, sent, received or otherwise used or relied upon for the provision of healthcare	PHI for which the healthcare organization is the originating party	Healthcare organization who receive access or correction requests involving PHI that originated at their organization	1. Respond to the request.
	PHI for which there is clearly a single creator/custodian	Healthcare organization who receive access or correction requests involving PHI that clearly originated from another healthcare organization	1. Direct the client to the originating party.
	Shared records	Healthcare organization who contributed PHI within their custody to a record that displays or is stored in a format where the record cannot be severed or where there is a compelling interest in providing the entirety of the record to the requestor.	1. Collaborate to provide a single point of access and answer questions. 2. Involve the HINP where needed for corrections. 3. Document access in the information repository, where possible.

4.5 PROCEDURE

4.5.1 RESPONDING TO ACCESS AND CORRECTION REQUESTS

CSC Chigamik CHC will follow their internal policies and procedures when responding to access and correction requests. Clients requesting to access their charts must fill out

Appendix M – Request for Access of Client Records and provide the completed form to the Privacy Officer.

Clients requesting a correction to their medical record must fill **Appendix N – Request for Correction of Client Records** provide the completed form to the Privacy Officer.

CSC Chigamik CHC policies and procedures are as follows:

1. Validate the identity of the requestor as the client who owns the information or as their SDM;
2. Determine whether the healthcare organization has authority to provide access to or correct the information. If the healthcare organization does not have authority to provide access to the information, the Privacy Officer will either direct the requestor to the appropriate organization or work with the Privacy Officers of the appropriate organizations to provide the individual with access;
3. Respond to requests when the information does not exist or cannot be found by providing written notice to the requestor;
4. To grant access, make the information available or make a copy of the information in cases where access is not subject to exemptions listed in PHIPA; and
5. To deny access, determine that a PHIPA exemption applies and provide a written response to the requestor.

5 RELEASE OF INFORMATION

5.1 PURPOSE

Clients have the right to have the confidentiality of their PHI maintained. The client's health record may be disclosed with the client's implied consent (as when agreeing to a referral), but in most cases will require express consent via submission in writing. The records are the property of the Centre. Originals shall not be released.

SDM for incapable clients can have access to client's health information to enable him or her to make an informed decision as to consent. Please refer to Clinic Policies – Informed Consent, "Who May Act as Substitute Decision Maker" which lists the hierarchy of individuals/agencies that can act as SDM.

The executor or administrator of the estate of a deceased client is generally entitled to have access to the client's record, upon showing documented proof of position.

When the person authorizing the release is not the client or SDM, a copy of the supporting legal documentation is required to be kept on file. This documentation includes but is not limited to: power of attorney, executor/estate trustee, litigation guardian, or custody (in the event of a separation, divorce or other guardianship issue).

All requests to release personal health information must be submitted in writing to the Privacy Officer using **Appendix M – Request for Access of Client Records**. A written authorization is required for each request.

Upon receipt of an authorized release of information, staff must ensure that the client (or guardian) has signed and dated the request, and that the signature has been witnessed. Only the specific information requested is forwarded. The information being released will be documented and kept on file.

5.2 POLICY

5.2.1 REFUSING OR SEVERING A RECORD

CSC CHIGAMIK will act in accordance with PHIPA, 2004 with regards to refusing or severing all or part of the requested record(s).

5.2.2 OVERRIDING CONSENT FOR THIRD-PARTY PHI DISCLOSURE

The client's PHI must be disclosed without the client's consent in the following cases:

- Responding to a subpoena (with legal advice);
- Preventing serious injury to others (duty to warn under common law);
- Reporting of communicable and reportable diseases (as required under the Health Protection and Promotion Act);
- Reporting child abuse (as required under the Child and Family Services Act);
- Reports in respect of an injured worker (upon written request of the WSIB);
- Reporting unfit drivers (as required by the Highway Traffic Act);
- Reporting unfit flight crew members, air traffic controller or other person holding a Canadian Aviation Document (as required by the Aeronautics Act);
- Sexual abuse by a Regulated Health Professions Act (RHPA) professional (Note: Client's consent is required for the disclosure of the client's name as required by RHPA); or
- Termination of suspension or employment, for reasons of professional misconduct, incompetence or incapacity (as required by RHPA).

When any of these circumstances arise, opinion of the Centre's legal counsel should be sought before acting on the external demand. When it is deemed to be an appropriate situation to override consent, the provider overriding consent must fill out **Appendix J – Consent Override Notification** and submit it to the Privacy Officer. **Appendix K – Consent Override Letter** will then be provided to the client explaining the situation in which their consent was overridden.

5.2.3 PRECAUTION RE: POLICE

Except in circumstances specifically described above, healthcare providers should not disclose to police, any information in the course of treating a client. Care should be taken, however, not to mislead or provide false information. In cases of doubt, the Centre's legal advice should be sought.

5.2.4 TRANSFERRING CLIENT FILES

PHI is transferred to another provider only with a written request from the client. **Appendix O – Consent to Disclose Personal Health Information** should be signed, dated, witnessed and will contain the name and address of the practitioner that the client is requesting the transfer to. This form should normally be sent from the doctor's office requesting the client's file. A verbal request is not sufficient to transfer client records.

The client should be encouraged to see their new primary care provider and sign a consent form with them for the release of information. If this is not possible, however, the client may sign a copy of **Appendix O – Consent to Disclose Personal Health Information.**

Originals are never sent as they are the property of the Centre and must remain accessible to Centre staff for at least 10 years after the date of the last entry in the record, or until 10 years after the day on which the client reached or would have reached the age of eighteen.

5.2.5 LAWYERS AND INSURANCE ADJUSTERS

Upon the authority of the Executive Director, client records should be provided to the Centre's own lawyer, own liability insurer or an adjuster or a lawyer acting on behalf of the Centre's insurer.

If legal action is taken, current and past employees of the Centre and their lawyers should have access to records of clients they have treated.

If a Lawyer or Insurance Adjuster representing the client would like to request client PHI, they are required to submit written consent from the client using either their own internal Release of Information form or **Appendix O – Consent to Disclose Personal Health Information.**

A fee will be charged to lawyers and Insurance Adjusters. See fee structure chart in Section 5.3.2 Charging Access Fees, for more details.

5.3 PROCEDURE

CSC CHIGAMIK CHC is responsible for responding to release of information requests pertaining to the PHI which it initially collected.

If the PHI being requested includes information that was originally collected by another provider, the Privacy Officer at the organization to which the request was made shall work with the Privacy Officer at the other organizations to provide the client with access to all or some of his or her PH

5.3.1 RESPONDING TO RELEASE OF INFORMATION REQUEST

When authorized persons request access to information using **Appendix O - Release of Medical Information Form**, CSC CHIGAMIK CHC shall:

1. Validate the identity of the authorized person and notify requestor of fee structure;
2. The health professional is most involved with the client's care should be consulted if possible, prior to the release of information. *Note – As records may be difficult to read and interpret and may mislead or alarm a client, the authorized person will be encouraged to review the records with their provider so the information can be explained.*
   *Exceptions – There may be special circumstances which warrant withholding information or records. In these cases, the provider will consult appropriately before deciding if the information and/or records should be released.
3. A notation shall be made in the records stating:
   - What information or records were disclosed;
   - When the information or records were disclosed; and
   - By whom the information or records were disclosed.
4. Respond to requests when the information does not exist or cannot be found by providing written notice to the requestor using **Appendix P – Denial of Access – Release of Information Notification.**

Reception staff will never dispense any information themselves, unless directed to do so by the Privacy Officer.

Counseling records are handled differently and can never be released in conjunction with other clinical records. Reception staff must be aware of this. Prior to releasing counseling records concerning a client, the counselor must secure written informed consent from the client. In addition, the client should be informed of any potential harm resulting from the release. Minimal information, addressing only those issues directly relevant to the request, should be provided.

5.3.2 CHARGING ACCESS FEES

This fee structure was developed provincially in accordance with Health Order-009 issued by the Information Privacy Commissioner of Ontario (IPC). This table was adapted from the North Simcoe Muskoka Community Care Access Centre (NSM CCAC) – Policies and Procedures Manual – Request to Release Personal Health Information to Client or Third Party – January 2013.

Requestor	Consent Required From	Fee
Client or SDM	Client or SDM	$30.00 for the first 20 pages and $0.25 per page thereafter
Lawyer, Legal Aid Clinic, Advocacy Centre	Client or SDM	$30.00 for the first 20 pages and $0.25 per page thereafter
Insurance Company	Client or SDM	$25 for a letter of confirmation of service. $30.00 for the first 20 pages and $0.25 per page thereafter $30 fee for results on CD, this does not include a $10 fee for the cost of the CD
Physician, Hospital or other Health Information Custodian	N/A if both HIC's are currently involved in the care of the client	No fee
	Client or SDM if either HIC is not involved in the care of the client	
Public Guardian and Trustee	N/A	No fee
Social Service Agencies, Child Protective Services	Client or SDM	No fee
Coroner	N/A	No fee
Court order, warrant, subpoena, or other process issued by court of Ontario	N/A	No fee
Police (without documentation listed above)	Client or SDM	No fee
Veteran's Affairs Canada	Client or SDM	No fee
Other government agencies	Depends on Request	No fee
Professional College (ex. College of Physicians and Surgeons of Ontario)	N/A	$0.25 per page (based on the maximum amount they are willing to pay
Criminal Injury Board	Client or SDM	$25 for a letter of confirmation of service. $30.00 for the first 20 pages and $0.25 per page thereafter

Workplace Safety Insurance Board (WSIB)	Client or SDM	$48.15 flat fee
Employer	Client or SDM	$25 for a letter of confirmation of service. $30.00 for the first 20 pages and $0.25 per page thereafter
Oxygen Supplier	N/A	No Fee

6 AUDIT LOGGING AND REPORTING

6.1 PURPOSE

To monitor access to PHI in the shared electronic service in order to facilitate investigations related to complaints about or known unauthorized access to PHI by authorized users and to identify potential privacy incidents.

To conduct routine reviews of compliance with policies and procedures related to the protection of the privacy and confidentiality of PHI.

6.2 POLICY

6.2.1 GENERAL

CSC Chigamik CHC shall audit the operations to ensure they meet with statutory requirements, privacy and security policies and procedures, and privacy benchmarks or standards established by the initiative.

PHI may be used for the purpose of risk management if appropriate safeguards are in place to protect the confidentiality of PHI, the PHI is used by or on behalf of the originating party, and any PHI that is contained in the shared service not intended for clinical purposes is destroyed immediately after use.

6.2.2 IDENTIFYING INAPPROPRIATE ACCESS

CSC Chigamik CHC shall examine audit log reports monthly, in conjunction with other available information, to identify and investigate unexplained or potentially inappropriate access to PHI in the shared service. Some indicators of unauthorized or inappropriate access include but are not limited to:

1. An end-user accessed the record of a client who did not receive care in the healthcare organization on the same day as the access occurred;
2. Where the access did not support a clinical or business-related function (note that anticipatory or delayed functions such as preparing records for upcoming appointments are acceptable);
3. End-user access to a record or part of record that has been blocked by a consent directive and where that access was conducted without the consent of the client;
4. End-user access to the record of a client with whom the user does not have an established patient-provider relationship;

5. An end-user accessed a record from an unexpected location (e.g. another healthcare organization site; non-authorized IP address); or
6. Other circumstances as dictated by specific concerns or unusual patterns of behavior (e.g. when an end-user has the same last name as the client whose record was accessed).

Any healthcare organization that discovers inappropriate access shall communicate this to other affected healthcare organizations and shall work to remedy the incident according to internal policies and procedures or, in cases where other healthcare organizations are involved, shall follow the Incident Management policy.

6.2.3 Provision of Audit Reports by External Party

A HINP is required by law to provide an audit report to participating healthcare organizations, at their request, that lists accesses to and transfers of the PHI which is held or transferred by and via the HINP's equipment.

The HINP will provide all participating parties with the following information when requested:

- A report of all active end-users associated with a particular healthcare organization to the Privacy Officer; and
- An audit report of all access by a healthcare organization's authorized users to any records/PHI of individuals whose PHI is retained in the HINP's external data stores and which are transmitted by the HINP.

Additional access reports will be provided upon request, and within a reasonable timeframe, such as in the instance of a reported or suspected privacy breach.

6.2.4 Technical Requirements for Audit Reports

The shared service shall produce standard user-friendly reports that facilitate the auditing activities required of healthcare organizations.

The reports may be tailored according to focus (i.e. which end-users engaged in which activities in a particular individual's record; which activities performed were performed in which individuals' records by a particular end-user), time period or other search criteria, where available. The following types of reports are available in the information repository to facilitate proactive/random and investigative audits:

1. Report of all access by all end-users associated with a particular healthcare organization to any and all client records:
    a. Displays which end users accessed particular records; and

b. Includes type of activity performed, and time/date stamp of each activity.

2. Report of all clients records which were accessed by a single end user:
    a. Displays which records the end user accessed; and
    b. Includes type of activity performed, and time/date stamp of each activity.
2. Report of all changes in consent directives:
    a. Display the patient and actions taken by the user; and
    b. Information about the user who made the change and time/date stamp of the change.
3. Report of all consent directive overrides:
    a. Display name of the client whose consent directive was overridden and the end-user who took the override action;
    b. Information whether the override was with or without consent, and, in the instance of override without consent, the reason provided by the user; and
    c. Includes the time/date stamp of all overrides.

6.3 RESPONSIBILITIES

CSC Chigamik CHC is responsible for on-going random quarterly auditing of the operations of their organization and the activities of their agents to ensure there has been no unauthorized or inappropriate access, use or disclosure of PHI.

The HINP is responsible for providing, upon request, a report of all accesses to part or all of a client's PHI associated with the shared service.

The HINP will provide ad hoc audit reports upon request of the healthcare organization for investigation of an incident, complaint, or concern, and will do so within a reasonable timeframe.

The HINP will produce and examine system audit reports related to information repository functionality and end-user management (e.g. unsuccessful login attempts) and report any identified concerns to participating healthcare organizations. Reports would be released to CSC Chigamik CHC on condition that the reports are kept confidential, retained according to the healthcare organization's internal policies, and not distributed outside of the organization, except where required by law.

It is the healthcare organization's responsibility to determine whether the reports suggest an actual or potential privacy incident or breach, and to address it according to the guidelines established within these policies and procedures.

Healthcare organizations must cooperate with each other to ensure that suspected or confirmed inappropriate access is investigated and addressed. The HINP shall cooperate with CSC Chigamik CHC during an investigation of potentially inappropriate access by verifying which, if any, end-users listed are HINP personnel providing legitimate support within the information repository.

6.4 PROCEDURE

6.4.1 INVESTIGATING UNEXPLAINED OR POTENTIALLY INAPPROPRIATE ACCESS

Where unexplained or inappropriate access to PHI under the custody or control of the healthcare organization by its agent is found, the healthcare organization should follow its internal policies and procedures of investigation and remediation.

Where unexplained or inappropriate access to PHI is identified by another healthcare organization:

1. The identifying healthcare organization will inform the affected healthcare organization(s) and/or HINP of the incident;
2. The affected healthcare organization will follow its internal procedure for investigating unauthorized access to PHI; and
3. The affected healthcare organization will communicate with the identifying healthcare organization about whether or not access was appropriate and, where required, how it will address the issue with the involved end-user and the client or their SDM.

Where unexplained or inappropriate access to PHI is identified by CSC Chigamik CHC please refer to Section 7: Privacy Incident Management.

7 PRIVACY INCIDENT MANAGEMENT

7.1 PURPOSE

To respond quickly and effectively to privacy incidents involving PHI contained in the shared information repository by following a process to monitor, report, contain, notify, investigate, and remediate an incident.

7.2 POLICY

CSC Chigamik CHC will ensure prompt investigation and containment and promptly report any complaints or breaches of confidentiality and/or security. Awareness of any such incidents may come directly from the affected person(s) or from other parties or from regularly scheduled privacy audits.

A privacy concern or complaint is not referred to as a breach until it has been proven to be otherwise.

Under Section 72(2)(3), if an offence is committed under PHIPA, every individual or HSP of the shared service who authorized the offence, or had the authority to prevent the offence from being committed and knowingly refrained from doing so, is a party to and guilty of the offence. The individual is liable, on conviction, to the penalty for the offence, whether or not CSC Chigamik CHC has been prosecuted or convicted.

7.2.1 CATEGORIZATION OF BREACHES

Categorization of breaches assists in standardizing sanctions. Privacy breaches are categorized in the following manner:

Category 1

Accidental or Inadvertent Violation – This is an unintentional violation of privacy or security that may be caused by carelessness, lack of knowledge, lack of training, or other human error. Examples include, but are not limited to:

- directing PHI via mail, email or fax to a wrong party;
- discussing patient information in public areas or within hearing range of other people who do not require access; and
- incorrectly identifying a patient record.

Category 2

Failure to follow established privacy and security policies and procedures – This is a violation due to poor job performance or lack of performance improvement. Examples include, but are not limited to:

- release of PHI without proper patient authorization;
- discussing PHI with another person who is not involved in the care of the patient or does not require the information to perform their job functions;
- leaving detailed PHI in a public area (e.g. photocopier, meeting room,)
- leaving detailed PHI on an answering machine;
- failure to report privacy and security violations;
- improper disposal of PHI;
- failure to properly sign off from, or lock a computer when leaving a workstation;
- failure to properly safeguard password(s);
- failure to safeguard the portable/mobile device(s) from loss or theft;
- failure to store PHI on unencrypted data capable devices (e.g. portable devices such as USB sticks, MP3, personal computers);
- transmission of PHI using an unsecured method;
- accessing one's own PHI rather than following requests for information policy and procedure; and
- failing to lock an office door that contains files with paper copies of PHI.

Category 3

Deliberate or purposeful violation without harmful intent – This is an intentional violation due to curiosity or desire to gain information for personal use. Examples include, but are not limited to:

- accessing the information of high profile people, family members, or staff who are or were patients/clients at the organization; and
- accessing or using PHI without a legitimate need to do so, such as checking for a record of a co-worker, family or friends.

Category 4

Willful and malicious violation with harmful intent or personal gain– This is an intentional violation causing patient/client or organizational harm (negative physical, emotional, social or financial impact to an individual). Personal gain is collecting, using or disclosing PI/PHI with a motive that primarily benefits the individual (e.g. favors, economic gain, social or personal interests, etc.) Examples include but are not limited to:

- disclosing PHI to an unauthorized individual or entity for illegal purposes (e.g. identity theft);
- posting PHI to social media websites;
- disclosing PHI to the media; and
- disclosing PHI or individual identifying information in non-sanctioned publications (e.g. auto-biography).

7.2.2 DUTY TO REPORT PRIVACY INCIDENT

A privacy incident occurs when a healthcare organization or one of its agents (users):

1. Has contravened or is about to contravene a provision of PHIPA or its Regulations;
2. Contravenes the privacy provisions of the DSA or collects, uses or discloses PHI in the shared service for purposes other than those described in the DSA (e.g., a healthcare organization uses PHI for purposes other than providing or assisting in the provision of client care or for PHIPA-authorized secondary purposes);
3. Believes or has reason to believe that PHI has been lost, stolen, or has been used, disclosed, copied or modified in an unauthorized manner;
4. Provides access to client's PHIPA the shared service to an individual who is not otherwise permitted to access the data;
5. Accesses client PHI in the shared service without a clinical relationship with that client; or
6. Contravenes a requirement set out in the confidentiality agreement with which the user has agreed to comply

Any person that becomes aware of a privacy-related incident has the duty to immediately report that incident to the organization's Privacy Officer. The Privacy Officer has the duty to investigate the incident and, where required, work with other organizations as part of the investigation, follow-up, mediation and response. This may include reporting the incident to the Information and Privacy Commissioner's Office.

Upon discovery of an actual or potential privacy incident, the organization shall act immediately to contain the incident to prevent further damage (see section below on confinement).

7.2.3 RISK RESPONSE

Depending on the severity of the incident, differing responses and investigative methods may be required.

7.2.4 NOTIFYING INDIVIDUALS

Where PHI is stolen, lost, or accessed by unauthorized persons, or collected, used or disclosed in a manner or for a purpose not permitted by PHIPA or the

DSA, the involved organization must notify the impacted individuals using **Appendix L – Privacy Breach Notification Letter**.

Involved persons may have unique responsibilities with respect to each step in the incident management process (ex. Privacy Officer may have a specific role in containing the incident whereas an end-user may have a specific role in documenting the incident).

7.3 RESPONSIBILITIES

CSC Chigamik CHC is responsible for training its end-users on how to recognize and report a privacy incident. CSC Chigamik CHC is also responsible for enforcing the incident management protocol and implementing and mitigation strategies for noncompliance. Should an incident / breach involve a patient whose PHI is a part of the shared services, it is the responsibility of CSC Chigamik CHC and / or the affected HSPs to report immediately to each other as the case may be if they become aware of:

- a public complaint or an awareness of potential or a suspected breach of PI or PHI;
- an incident regarding unauthorized collection, use or disclosure of PI or PHI;
- any compromise of confidentiality and security of information, or security systems containing PI or PHI;
- an allegation of a privacy breach where the allegations have not yet been substantiated or refuted by investigation; and
- Participate in the investigation and management of a privacy breach with appropriate representation, as applicable.

The Privacy Officer (or delegate) will promptly contain the incident and initiate an investigation of the complaint or incident and compile the facts according to procedure.

Upon learning of a privacy breach or being alerted to a patient's concern regarding the security of his or her personal health information, employees and affiliates must immediately contact the Privacy Officer. Whistleblowers are protected under the Whistleblowing Protocol policy and the Personal Health Information Act (2004) from any reprisal for having made in good faith a disclosure, and will be protected if the employee:

- Discloses the info in good faith
- Believes it to be substantially true
- Does not act maliciously or make false allegations; and
- Does not seek any personal or financial gain

Each healthcare organization is expected to work with other healthcare organizations affected by or otherwise involved in the privacy incident to investigate and resolve the incident. These organizations and/or the HINP may be required to participate in the reporting of a privacy incident to the Information and Privacy Commissioner.

7.4 PROCEDURE

7.4.1 MONITORING FOR INCIDENTS

CSC Chigamik CHC must monitor their agents' activities to ensure PHI in the shared service is collected, used, and disclosed within the terms and conditions of the DSA and in compliance with PHIPA.

Monitoring activities should be overseen by each healthcare organization's Privacy Officer and should include:

1. Reviewing information repository audit log reports for unusual or unauthorized activities;
2. Reviewing the list of authorized agents with access to the information repository to ensure the list is up to date (e.g., agent roles and responsibilities have not changed);
3. Reviewing reports that detail changes to consent directives;
4. Reviewing consent overrides (with and without consent) to confirm appropriateness of the action; and
5. Receiving, investigating and reporting on privacy complaints made by clients or SDMs, the public, and healthcare organization staff.

Frequency of monitoring will take place on a monthly basis.

7.4.2 REPORTING INCIDENTS

Agents are responsible for immediately reporting privacy incidents or suspected privacy incidents to their Privacy Officer (or to their incident manager or administrator-on-call, if after hours). Reporting of privacy incidents will be done using **Appendix D – Privacy Incident Report Form.**

The Privacy Officer (or designate, as required) is responsible for reporting the following to any other affected healthcare organization or the HINP at the first reasonable opportunity and, at maximum, within 24 hours:

1. the date and time the incident occurred;
2. a general description of the incident; and

3. the immediate steps that will or have been taken to contain and remedy the incident (see steps under "Containing Incidents" and "Remediating Incidents" respectively, below).

To ensure investigation, remediation, and notification activities are conducted in an efficient and appropriate manner, the parties involved in the incident will identify an Incident Lead (a single healthcare organization to lead the incident management activities). Generally, the incident response will be led by the Privacy Officer from the healthcare organization where the incident originated, unless otherwise decided by the consensus of the impacted healthcare organizations.

Notification to affected clients should be made by the impacted HIC where only one HIC is involved or through mutual consensus of the impacted organizations where multiple organizations are involved. Where possible, the HIC with the closest relationship to the client should provide the notice if it is impacted by the incident. Impacted HICs will cooperate with the Incident Lead, as appropriate, during each of the following stages.

Depending upon the circumstances surrounding the privacy incident, the Incident Lead may report the incident to:

1. The Information and Privacy Commissioner when the Lead, in consultation with affected healthcare organizations, determines that notification of the IPC is appropriate or required; the IPC's assistance is required to resolve the incident; or, the incident may otherwise come to the attention of the IPC;
2. Law enforcement, if theft or another crime is suspected (e.g., identity theft);
3. Technology vendors or suppliers that may need to assist in incident containment and resolution and prevention of future incidents;
4. Professional or regulatory bodies responsible for disciplining individuals involved in the incident and/or that require notification; or

The incident may be reported to end-users and/or other members of an affected healthcare organization's organization where their involvement is needed to appropriately address the incident. The privacy incident and the results of the investigation of the privacy incident should inform future privacy and security training within the initiative and to change existing policies and procedures as required.

7.4.3 CONTAINING INCIDENTS

The Privacy Officer must take steps to determine the scope of the incident and contain it. Containment includes preventing additional records of PHI from being affected as well as ensuring affected records are not further compromised by taking steps such as:

- Complete the form **Appendix D – Privacy Incident Report Form.**
- Initiate steps to contain the PI/PHI associated with the complaint or incident
- Promptly retrieve any hard and soft copies of any PI/PHI that has been made, retained or disclosed by an individual who was not authorized to receive the PI/PHI and obtain the person's contact information in the event that follow up is required
- Obtain assurances from unintended information recipients that they will not further collect, use, share or distribute the PI/PHI
- Determine whether the event would allow unauthorized access to other PI/PHI and take necessary steps that are appropriate to contain the event
- During the investigation in consultation with Human Resources and the individual's Manager, mitigation measures may be taken to ensure that the individual is removed or access is limited from any area or work task that could enable any further breaches.

Containment should occur as soon as reasonably possible and should take into consideration the actual or potential severity of the incident (i.e., where a larger number of individuals are affected or sensitive information is involved, CSC Chigamik CHC should respond faster). To ensure timely action is taken, it is imperative that all users and accountable persons are trained in how and when to implement the protocol.

Containment is considered complete when PHI that is the subject of the privacy incident and/or other PHI is no longer at risk of inappropriate collection, use, disclosure or access.

7.4.4 NOTIFYING INDIVIDUALS OF INCIDENTS

CSC Chigamik CHC is required to notify individuals whose PHI was stolen, lost, or accessed by unauthorized persons, as well as collected, used or disclosed in a manner or for a purpose not permitted by PHIPA. If the investigation determines that a privacy breach occurred, the Privacy Officer will notify the appropriate individuals within the organization (e.g. Executive Director.). With respect to individuals within the Regulated Health Professions Act, a consult will be had with Human Resources who will collaborate with the appropriate

organizational leadership for the purpose of notifying the individual's Regulatory College.

The IPC may be contacted outlining the breach, steps taken and the notification process to the patients. If, in consultation with the IPC, it is determined that a breach necessitates police notification, then this will be carried out.

Prompt steps will be taken to notify affected persons or their substitute decision maker (SDM) in accordance with PHIPA except where there are exceptional circumstances (e.g., notification is not possible or may be detrimental to the individual as determined in consultation with clinical staff). Notification is handled by the most appropriate person in consultation with the Privacy Office. Notice can be completed by telephone or in person and followed with a written notice using **Appendix L – Privacy Breach Notification Letter**. The notice will include:

- Details of the nature and scope(e.g. date and time) of the breach and the particular PI/PHI at issue
- The measures implemented to contain the privacy breach and to prevent similar privacy breaches in the future
- The name and contact information for the person (i.e. Privacy Officer) to whom the individual may address inquiries and concerns;
- Apologize on behalf of the organization and provide the re-assurance that the organization takes the privacy of the individual's information very seriously. Include the fact that IPC has been contacted.
- The CSC Chigamik CHC controlled document, **Appendix L – Privacy Breach Notification Letter** should be used whenever possible. If this document is not used, the Privacy Office (or designate) shall provide a note in the investigation file explaining why an alternate letter was used.

7.4.5 INVESTIGATING INCIDENTS

The Incident Lead will conduct an investigation into all reported privacy incidents to:

1. Determine the cause and scope of the incident;
2. Ensure containment was successful;
3. Evaluate the adequacy of administrative, technical, and physical safeguards; and
4. Develop and implement remediation activities to prevent future incidents.
5. The investigation could include a review of audit logs, reports, personal interviews, review of camera footage, paper records, communication system logs, Human Resources files, technology access systems, etc.

6. Complete the CSC Chigamik CHC controlled document, **Appendix L – Privacy Breach Notification Letter**
7. Based on the results of the investigation recommended improvements regarding information handling practices/procedures or security processes would be implemented

Reporting of the above information will be done using **Appendix D – Privacy Incident Report Form.**

7.4.6 RESULTS OF INVESTIGATION

If the investigation determines that a breach occurred the Privacy Officer will assign an appropriate category breach level and will collaborate with Human Resources and the individual's Manager to determine the discipline to be applied. In the case of a credentialed staff, the appropriate discipline will be determined in alignment with organizational practice. Discipline will be in accordance with the category breach level and will range from re-education up to termination of employment.

The Privacy Officer must provide a copy of **Appendix L – Privacy Breach Notification Letter** to the Privacy Officers of all affected healthcare organizations and if applicable to the HINP once the investigation is complete or within one month following the incident, whichever is sooner.

CSC Chigamik CHC agrees to fulfill reasonable requests for detail regarding the steps taken to address the incident and minimize the risk of recurrence.

CSC Chigamik CHC will respect the confidentiality of personal information pertaining to any disciplinary action that has been taken.

7.4.7 REMEDIATING INCIDENTS

The Privacy Officer must establish a remediation plan to address the cause of the incident and to ensure identical or similar incidents do not recur. A remediation plan should include:

1. A detailed description of the remediation activity (e.g., a review of relevant information management systems, any amendments or reinforcements to existing policies and/or practices, development and implementation of new security or privacy measures, testing and evaluating remedial plans and training of staff);
2. The individual(s) responsible for implementing the remediation activity;
3. The implementation schedule (i.e., when the implementation will be complete); and,

The healthcare organization responsible for the incident (or the Incident Lead, where appropriate) must report the completion of the remediation activities to the Privacy Officers of the affected healthcare organizations, and to the HINP Privacy Officer, who will track all privacy incidents involving the information repository in order to help determine system enhancements that can improve the protection of PHI.

Within CSC Chigamik CHC, the remediation plan is as follows:

- The Privacy Officer will regularly audit the access to PI and PHI of staff members who have been involved in privacy investigations for at least up to a period of one year after the breach.
- Implement approved steps to address/prevent future occurrences. This could include:
    - Review of Policies and Procedures:
        - Make recommendations with respect to the related information handling practices/procedures or security processes, including any improvements for protecting PI/PHI
- Staff Training:
    - Ensure staff are appropriately educated and trained with respect to compliance with organizational policies and directives regarding PI/PHI.
    - If the type of breach is not included in organizational orientation training, then add it.
    - Arrange for a formal communication to come from the Executive Director`s office.
    - Develop a strategy for ensuring the breach does not re-occur.
    - Limit access where appropriate.

8 INQUIRIES AND COMPLAINTS

8.1 PURPOSE

To respond, in a timely manner, to inquiries or complaints from clients, their SDMs, or members of the public regarding PHI in the shared information repository or the privacy and security of their PHI

8.2 POLICY

8.2.1 GENERAL

Individuals, their SDMs, or members of the public may challenge healthcare organizations' compliance with healthcare organizations' information management practices and with the provisions of PHIPA and its Regulation.

Individuals or their SDMs may issue an inquiry or complaint directly to the care provider/healthcare organization with which they have a clinical relationship and which has custody or control over their PHI.

Individuals, their SDMs, or members of the public may issue a complaint to the IPC if resolution of the inquiry or complaint by the healthcare organization is not satisfactory.

8.2.2 RESPONDING TO CHALLENGES INQUIRIES OR COMPLAINTS

CSC Chigamik CHC Privacy Officer will respond to inquiries or complaints from individuals, their SDMs, or members of the public on behalf of the organization and with respect to this initiative.

Upon receipt of the inquiry or complaint, each healthcare organization will confirm that it is the appropriate party to receive the inquiry or complaint and, where is it not, redirect the matter to the appropriate healthcare organization immediately. We ask that CSC Chigamik CHC clients use **Appendix E – Privacy Complaint Form** when launching a formal complaint.

Where the inquiry or complaint involves two or more healthcare organizations, a Response Lead will be chosen by consensus of the affected parties.

Where challenges, inquiries or complaints pertain to the shared service and/or the access to and use of the PHI within it, CSC Chigamik CHC will follow the procedures outlined below.

Complaints shall be documented by CSC Chigamik CHC by scanning in a copy of the complaint to the clients chart.

8.2.3 COOPERATING WITH AN IPC INVESTIGATION

If the IPC decides to investigate a complaint, CSC Chigamik CHC will cooperate with the process.

Cooperating with the process may include:

1. Cooperating with an investigation, including providing assistance that is reasonably necessary, such as using a device or system to produce a record in readable form;
2. Preparing and submitting written representations on the issues surrounding the complaint by the date stipulated by the investigator, or as soon thereafter as reasonably possible;
3. Providing comments to the investigator about the content of a draft order, which the investigator may prepare after reviewing written representations of all parties to the complaint; and
4. Complying with the investigator's final order, including addressing recommendations received.

Where two or more healthcare organizations are contacted by the IPC, the affected healthcare organization(s) may choose a Response Lead (by consensus) who will assist the IPC in each stage of the process and through whom select information may be communicated between CSC Chigamik CHC and the IPC.

8.3 RESPONSIBILITIES

Each healthcare organization is responsible for responding to inquiries or complaints as they relate to the healthcare organizations' use of the information repository to the best of their ability, according to the healthcare organizations' policies and procedures.

When inquiries or complaints are directed to, or involve, more than one healthcare organization, all affected healthcare organizations must cooperate to address the inquiry or complaint appropriately, including determining which healthcare organization will assume the responsibilities of the Response Lead. These responsibilities include coordinating activities and communicating with the inquirer/complainant.

If applicable, a HINP will work with a HIC to respond to inquiries and complaints relating specifically to the HINP's handing of PHIPA will provide information to a healthcare organization for use by the healthcare organization in responding to an inquiry or complaint.

In the case that the inquiries or complaints only directly affect CSC Chigamik CHC, the policies and procedures outlined in the Clinic Policy Manual will be followed.

8.4 PROCEDURE

8.4.1 RESPONDING TO AN INQUIRY OR COMPLAINT

CSC Chigamik CHC or Response Lead will respond to a privacy inquiry or complaint according to the following steps. Note that if, during the course of the investigation, a privacy incident is discovered, the Incident Management Policy (refer to Section 7 of this document) must be followed.

1. Review the completed **Appendix E – Privacy Complaint Form**
2. Determine the complexity, urgency and seriousness of the inquiry or complaint, estimated response time, and whether an investigation must be undertaken.
3. Acknowledge receipt of the inquiry or complaint and advise the individual of the anticipated response time. Whenever possible, straightforward questions should be responded to immediately (e.g., requests for a copy of a public notice).
4. Prepare an appropriate response to more complex inquiries or complaints (e.g., through a meeting, phone call or letter) and advise the inquirer or complainant, accordingly.
5. Where an investigation must be undertaken to address the inquiry or complaint, prepare an investigation plan, which should include:
    - The areas that must be investigated;
    - The resources required to perform the investigation (internal and external);
    - The estimated duration of the investigation;
    - The plan for cooperative and consultative activity; and
    - The plan for communicating the status and results of the investigation.
6. Conduct the investigation and summarize the findings in a report to be provided to the individual who made the inquiry or complaint. Follow up with the inquirer or complainant as appropriate (e.g., through a meeting, phone call or letter).

9 TRAINING

9.1 PURPOSE

9.1.1 To assist CSC Chigamik CHC in ensuring their employees, contract staff and agents (end-users) are knowledgeable about their responsibilities related to protecting client privacy and PHI in the shared service.

9.2 POLICY

CSC Chigamik CHC have the responsibility to appropriately inform their employees, contract staff and agents / end-users of their obligations and responsibilities under PHIPA to protect the privacy and confidentiality of PHI they collect, use and disclose.

There may be privacy or security issues related to the shared service that are not addressed by an organization's standard privacy and security training program. CSC Chigamik CHC must ensure that their end-users receive privacy and security training specific to the shared service before being provided access. This training must be refreshed annually, and particularly when significant changes to the system are introduced or when a new PHIPA Order is released that will impact the data / PHI protection and security processes currently in place.

CSC Chigamik CHC must ensure end-users with access to the shared information repository are sufficiently trained in information repository-specific privacy topics including:

1. The purposes for the collection, use, and disclosure of PHI via the information repository
2. The circumstances under which implied consent is adequate or express consent is required
3. How to manage consent and consent directives (e.g., withdrawal) in the shared service
4. How to respond to (granted) requests for access and correction of client PHI that has been collected by another or more than one healthcare organization;
5. The physical, technical, and administrative safeguards employed to protect the PHI in the shared service;
6. How to respond to and forward public inquiries and complaints about information management related to the initiative; and

7. How to identify potential or real privacy incidents involving the shared service

Specific training at the time of employment and before access to PHI shall include the following:

Phase 1 completed on or before entering / working in the workplace.

a) Viewing the video provided by the AOHC on Privacy within our Organization as well as completing the quiz that accompanies.
b) Reading the guide produced by PHIPA entitled, "*PHIPA Guide to Privacy."*
c) Reading and signing the **Appendix Q – Statement of Compliance with Confidentiality, Privacy and Security Requirements.**

Phase 2 completed within two weeks of entering in the workplace.

a) Hands-on by a designated privacy trainer, CSC Chigamik CHC specific policies and procedures applying to PHIPA and PHI, along with a facility walk-through and discussion of specific areas of potential breach, location of PHI, questions and answers related to PHI and PHIPA.

Where specific job functionality exists, such as for electronic records management or use, training will include information specific for each employee to ensure that end-users are aware of all technical steps required or available to complete each task.

Appendix Q - Statement of Compliance with Confidentiality, Privacy and Security Requirements informs end-users of their specific obligations to protect the privacy and confidentiality of client PHI when using the shared service and the PHI contained therein.

All signed **Appendix Q - Statement of Compliance with Confidentiality, Privacy and Security Requirements** and confirmation of training records shall be retained as part of the end-user's personnel record.

9.3 RESPONSIBILITIES

CSC Chigamik CHC is responsible for providing information on the shared service -specific privacy and security practices and safeguards for maintaining the confidentiality of PHI contained in or transported by shared information systems.

CSC Chigamik CHC is responsible for ensuring that appropriate training materials and topics are delivered to end-users prior to gaining access to the shared service and upon changes to the functionality of the shared service. CSC Chigamik CHC is responsible for ensuring all users sign **Appendix Q -**

<<Initiative Name>>

Statement of Compliance with Confidentiality, Privacy and Security Requirements prior to being given access to the shared services.

10 RELEVANT AUTHORITIES

Personal Health Information Protection Act, 2004 (PHIPA)

Ontario Regulation 329/04 made under the *Personal Health Information Protection Act, 2004*

Below are the legislative and regulatory sections pertaining to the particular sections of this document:

Consent (policy): PHIPA s. 3(1), 20(2), 37(1)(a), 38(1)(a) and 50(1)(e)

Access and Correction (policy): PHIPA s. 52 and 55

Access and Correction (charging access fees): PHIPA s. 54(10) and (12)

Access and Correction (responding to access requests): PHIPA s. 55(1) and (8)

Auditing (policy): PHIPA s. 12, s. 13, s. 34 and s. 37,; O. Reg. 329/04 s. 6

Incident Management (policy): PHIPA s. 12(1) and (2)

Incident Management (responsibilities): PHIPA s. 15(3)(b)

Incident Management (notifying individuals of incidents): PHIPA s. 12(2)

Inquiries and Complaints (policy): PHIPA s. 15(3), s. 56 and s. 58

Inquiries and Complaints (procedure: cooperating with an IPC investigation): PHIPA s. 60(8) and s. 61(1)

Training (policy): PHIPA s. 15 (3)(b)

PHIPA Order HO-013, December 16, 2014