COMMUNITY HEALTH CENTRES OF NORTHUMBERLAND

Policy and Procedure Manual

Topic: Privacy					
Section: Organizational					
Cross Reference: Client Health Record Documentation					
Relevant Legislation: PHIPA, 2016					
Original date: June 2010 (Previously called the Protection of Personal and Personal Health Information					
Approved by: Privacy Committee/Privacy Officer					
Reviewed/Revised Dates					
Date: May 2012	**Date:** June 2016	**Date:** April 2018	**Date:**	**Date:**	**Date:**
Initial: J.H.	**Initial:** L.T.	**Initial: L.T.**	**Initial:**	**Initial:**	**Initial:**
Date of next review: April 2020					
Person Designated to ensure revision and adherence: Privacy Officer					

Purpose: To provide the Community Health Centres of Northumberland (CHCN) with the necessary direction on the collection, use, retention, transfer and disclosure of client information both inside and outside of the organization.

Policy and Procedures: included in this document:

- Access and Correction
- Inquiries and Complaints
- Privacy Breach Management
- Privacy and Security Training
- Consent Management
- Logging and Auditing
- Retention

Supporting Operating Practices
Supporting Tools and Templates
Glossary of Terms

Access and Correction Policy and Procedure - PHIPA Reference: Sections 51-55

Templates or forms associated with these Procedures:

- **Request for Access Form**
- **Request for Access Log**
- **Response to a Request for Access Form**
- **Request for Correction Form**
- **Request for Correction Log**
- **Response to a Request for Correction Form**
- **Notification of a Request for Correction to other HICs Template**

1. Policy:

Clients may ask to see or get copies of their medical records. They can ask us verbally or make a written request.

Clients may ask The CHCN to correct their medical records if the information is out-of-date, inaccurate, or incomplete.

The CHCN must respond to all requests to see, get a copy of, or to correct the medical record within 30 calendar days. The CHCN must notify the client that we require an additional 30 calendar days to respond if:

1.1. Responding within 30 calendar days would interfere with normal clinic functioning because finding or compiling the medical record is very complex; or

1.2. More time is needed to confirm whether some of the medical record should be withheld.

The CHCN may decide not to make a correction to a medical record if:

1.3. The information was received from another organization and The CHCN does not have enough information to know whether it should be corrected;

1.4. The correction is frivolous, vexatious, or requested in bad faith;

1.5. The medical record is not incorrect or incomplete; or

1.6. The information represents a clinical opinion that was made in good faith.

If the client asks, The CHCN must note in the medical record if the client asked for a correction but The CHCN refused to make the correction.

The CHCN may decide not to release some or all of the medical record if there is a good reason. The reason must be consistent with PHIPA s52.

2. Procedures:

When a client asks a clinician to see or get a copy of the medical record, the clinician should show or create a copy the medical record if it is easy to do (e.g., showing the client your screen, printing the medical record from the electronic medical record).

If the clinician cannot show or give a copy of the record to the client, the clinician must give the request to The CHCN privacy officer.

When the client asks an administrative staff member or makes a written request

Step 1. The administrative staff member who receives the request must:

1.1. Try to get enough information from the client to be able to identify the medical record he or she needs; and

1.2. Give the request to The CHCN privacy officer.

Before giving the client his or her medical record, The CHCN privacy officer must:

1.3. Write in *Request for Access Log* that the request was made;

1.4. Verify the identity of the client by asking for photo identification or by asking another member of the clinic, if The CHCN privacy officer does not know the client;

1.5. Confirm that the person is indeed the substitute decision maker for the client, if applicable, by following the Guidelines for Identifying a Substitute Decision Maker;

1.6. Identify any location or system (e.g., paper, EMR) where the client's medical record exists;

1.7. Confirm with the client's clinicians whether any information in the medical record should not be given to the client (see the possible reasons in Policy #6 above);

1.8. Tell the client how much they will be charged, if any, to give him or her a copy of the medical record; and,

1.9. Direct the client to contact relevant program office (e.g. eHealth Ontario) to make the Request for Access if the medical record involves PHI contributed by another organization, or involves logs to which the HIC has no access.

When responding to the client, The CHCN privacy officer must do one of the following:

1.10. Give a complete copy of the medical record;

1.11. Give only some of the medical record if PHI (see the possible reasons in Policy #4 above for not giving all of the information);

1.12. Not give any information from the medical record (see the possible reasons in Policy #4 above for not giving all of the information); ***or***

1.13. Notify the client in writing that The CHCN needs another 30 days to respond (see the possible reasons in Policy #3 above for needing more time).

If The CHCN only releases some information or needs more time, The CHCN privacy officer must complete the relevant *Request for Access Response Template*.

The CHCN privacy officer or designate must meet with the client to explain any abbreviations, terminology, or codes if the client asks.

The CHCN privacy officer must log the results of the request using Request for Access Log.

Charging Fees

Step 1. The CHCN privacy officer must:

1.1. Decide whether to charge or waive a fee to cover the cost of printing the medical record.

1.2. Ensure that the client is told the fee before preparing the medical record and not change it after the client has agreed to the fee.

Correcting the Medical Record

Step 1. The client must:

1.1. Complete the *Request for Correction Form* to ask to correct his or her medical record.

The CHCN privacy officer or designate must:

1.2. Help the client to complete the form if necessary;

1.3. Discuss the correction with the appropriate clinician(s) to determine whether to change the information; and

1.4. Respond to the request within 30 days of having received the request.

When responding to the client, The CHCN privacy officer must do one of the following:

1.5. Make the correction;

1.6. Notify the client that the request has been refused (see the possible reasons in Policy #4 above for not making a correction); or

1.7. Inform the client that an additional 30 days is required to respond to the request.

If the correction is granted, The CHCN privacy officer or designate must:

1.8. Strike out the previous information in the medical record (leaving it readable) and record the new information as soon as possible.

1.9. Upon request from the patient, inform any other clinics or healthcare providers to which The CHCN disclosed the information of the change if it may impact the client's care[1].

If the correction is refused, or more time is required, The CHCN privacy officer must complete the *Request for Correction Response Template* and ask the client whether they would like to attach a note to his or her medical record explaining that he or she disagrees with the accuracy of the information.

Receiving Requests for Access or Correction related to Shared Systems (e.g., Connecting Ontario)

Step 1. If the client requests to view or get a copy of their medical record in a shared system, The CHCN privacy officer must:

1.1. Follow these procedures (i.e., starting at number 1 of this operating practice) if the medical record was contributed by the clinic; or

1.2. Give the client contact information within 30 days for the program office responsible for the shared system (e.g., eHealth Ontario) if the medical record was contributed by another or multiple clinics.

If the client asks for a correction to a medical record in a shared system, The CHCN privacy officer must:

1.3. Follow these procedures (i.e., starting at number 1 of this operating practice) if the medical record was contributed by the clinic; or

[1] To facilitate with this request, submit an Audit Report Request to eHealth Ontario to request a report detailing which other HICs have accessed the patient's health record.

1.4. Give the client contact information within 30 days for the program office responsible for the shared system (e.g., eHealth Ontario) if the medical record was contributed by another or multiple clinics.

If The CHCN receives a request from the program office on behalf of a client, it must follow instructions from the program office on whether to follow The CHCN's policies and operating practices to address the request or the policies and procedures governing the shared system.

Inquiries and Complaints Policy and Procedure - PHIPA Reference: s15 (3)

Templates or forms associated with these procedures:

- **Inquiry and Complaints Log**
- **Inquiry or Complaint Response Template**

1. Policy:

1. The CHCN allows clients to ask questions or make a complaint about its PHI handling practices or its compliance with PHIPA and the associated regulations. Inquiries or complaints may be verbal or in writing.
2. The CHCN must respond to all inquiries or complaints within 30 calendar days. In limited circumstances, The CHCN can notify the client that it requires an additional time to respond to an inquiry or complaint.

2. Procedures:

Inquiries or Complaints

Step 1. When a staff member receives a privacy-related question that is easy to answer, s/he should answer it.

If the staff member is unable to answer the question s/he must:

1.1. Tell the client that s/he will give the question to The CHCN privacy officer and that The CHCN privacy officer will respond within 30 days; and

1.2. Give the Inquiry to The CHCN privacy officer

If a clinical or administrative member receives a privacy-related complaint s/he must:

1.3. Tell the client that s/he will forward the complaint to The CHCN privacy officer and that The CHCN privacy officer will respond within 30 days; and

1.4. Give the Inquiry to The CHCN privacy officer

When receiving the question or complaint, The CHCN privacy officer must:

1.5. Contact the person within 30 days and ask for clarification if the question or complaint is unclear;

1.6. Ask the person to contact the appropriate organization if the question or complaint relates to them; and

1.7. Log that the inquiry or complaint was received using the Inquiries and Complaints Log.

When responding to the question or complaint, The CHCN privacy officer must:

1.8. Write a response to the question or complaint;

1.9. Circulate the response to other members of the clinic if required;

1.10. Respond to the question or complaint within 30 days or inform the person that an additional 30 days is needed; and

1.11. Update the *Inquiries and Complaints Log* when the response is sent.

When an Inquiry or Complaint Identifies a Breach

Step 1. If a question or complaint causes The CHCN to identify a privacy breach, it must follow Privacy Breach Management Policy.

Inquiries and Complaints Related to Shared Systems

Step 1. If a person has a question or complaint related to a shared system, The CHCN privacy officer must:

1.1. Respond to the question following normal procedures (i.e., starting at number 1 of this operating practice) if the answer is known; or

1.2. Give the client information within 4 days on how to contact the program office responsible for the shared system (e.g., eHealth Ontario) if it relates to the shared system or one or more other health service providers.

If The CHCN receives a question or complaint from the program office on behalf of a client, The CHCN privacy officer must follow instructions from the program office on whether to:

1.3. Respond to the person directly; or

1.4. Give the program office the information needed to respond.

Privacy Breach Management Policy and Procedure

Templates or forms associated with these procedures:

- Privacy Breach Log
- Privacy Breach Report

1. Policy:

1. The CHCN must promptly respond to any real or suspected privacy breaches.
2. All members of the clinic must support the privacy breach response if required by The CHCN privacy officer.
3. Willful privacy breaches or repeated instances of accidental privacy breaches caused by a member of the clinic will result in disciplinary action up to including dismissal and reporting to legal or regulatory authorities.
4. A privacy breach is:
   4.1. Any event where client information is collected, used, or disclosed counter to PHIPA, The CHCN's policies, or obligations defined in agreements binding The Port Hope Northumberland Community Health Centre.
   4.2. Any event where a client's privacy rights under PHIPA, The CHCN's policies, or agreements binding The CHCN are breached.

2. Procedures:

Responding to a Breach

Step 1. The person who identifies a suspected or real breach must:

1.1. Take immediate steps to prevent any further harm or risk; and

1.2. Inform The CHCN privacy officer of the suspected or real breach within one hour of identifying the breach.

The CHCN privacy officer must confirm whether the suspected breach is real.

The CHCN privacy officer must review the steps to ensure that no further harm or risk is anticipated.

The CHCN privacy officer has authority to take further action to minimize harm or risk up to and including:

1.3. Removing the person's access to any paper or electronic copies of medical records, including shared systems;

1.4. Retrieving any copies of PHI that were inappropriately collected, used, or disclosed;

1.5. Disconnecting systems from the network or Internet;

1.6. Requiring support from other members of the clinic to effectively contain the privacy breach; and

1.7. Taking any reasonable action to minimize harm or risk to a client or clients.

Once contained, The CHCN privacy officer must lead a breach investigation which includes:

1.8. Assembling members of the clinic as required to understand who was responsible for the breach and how it occurred;

1.9. Whether the breach was willful or accidental;

1.10. Whether other steps could be taken to minimize harm or risk;

1.11. The client or clients that were impacted by the breach; and

1.12. Recommendations to prevent further of the same nature breaches.

The CHCN privacy officer must document the breach and investigation using the Privacy Breach Report Template.

The CHCN privacy officer must report the breach to the Program Office responsible for the shared system if the breach involves a shared system (e.g., report to eHealth Ontario if it involves the Connecting Ontario Solution).

The Port Hope Northumberland CHC Executive Director must review the recommendations and determine which recommendations should be implemented.

The CHCN privacy officer must develop a plan to implement the approved recommendations and provide status updates to The Port Hope Northumberland CHC Executive Director as often as required.

The CHCN privacy officer must log the breach and resulting investigation using Privacy Breach Log.

Disciplinary Action

Step 1. Where the privacy breach was willful or is accidental, The CHCN privacy officer must make recommendations to The Port Hope Northumberland Executive Director.

Disciplinary action may include:

1.1. Remedial training;

1.2. Termination;

1.3. Restricted access to medical records;

1.4. Probation;

1.5. Reporting to Information and Privacy Commissioner of Ontario, the appropriate regulatory college, and/or law enforcement; and/or

1.6. Other disciplinary action as appropriate.

Notification to the Impacted Client(s)

Step 1. The CHCN privacy officer or designate must notify impacted clients of the privacy breach as soon as possible if their medical records have been collected, used, or disclosed counter to PHIPA, The CHCN's policies, or obligations defined in agreements binding The Port Hope Northumberland Community Health Centre.

The CHCN privacy officer or designate must notify clients of the privacy breach in a way that is sensitive to the needs of the client. Potential mechanisms to notify the client are:

1.1. Writing a letter;

1.2. Telephoning;

1.3. Putting a note in the medical record to speak with the client on his or her next visit; or

1.4. Public notices if the identity of the impacted clients is not known.

The CHCN privacy officer must work with clinic staff to determine the most appropriate way to notify clients, but the notice must generally include:

1.5. The name of the person or people who caused the privacy breach if it was a willful act or relevant to the privacy breach;

1.6. The date and time of the privacy breach;

1.7. A description of the nature and scope of the privacy breach;

1.8. A description of the PHI and scope of PHI that was breached;

1.9. What was done to contain the breach;

1.10. Summary of the investigation;

1.11. Steps that the impacted client(s) can take to protect their privacy or minimize the impact of the Privacy Breach, if applicable;

1.12. Contact information for The CHCN privacy officer ; and

1.13. Information about making a complaint to the Information and Privacy Commissioner of Ontario.

The CHCN privacy officer must save a copy of the notice provided to the impacted clients or log that the notice was given using Privacy Breach Log within 1 day of notifying clients.

Breaches Related to Shared Systems

Step 1. If the privacy breach relates to a shared system, The CHCN privacy officer must notify the program office responsible for the shared system by the end of the next business day after identifying the privacy breach.

Step 2. If the privacy breach is related to a shared system, The CHCN must follow instructions from the program office on managing the privacy breach, understanding that remediation or disciplinary activities must be approved by the applicable oversight body at the program office responsible for the shared system.

Privacy and Security Training Policy and Procedure - PHIPA Reference: Section 15 (3)

Templates or forms associated with these procedures:

- **Privacy eLearning Modules**
- **Training Log**

1. Policy:

1. The CHCN must appoint a person who is responsible for training clinical and administrative staff members on their privacy and security duties.
2. The CHCN must train all clinical and administrative staff members of their privacy and security obligations before giving them access to personal health information.
3. The CHCN must train them of their obligations on an annual basis.
4. All clinical and administrative staff must agree to their privacy and security obligations before getting access to personal health information and on annual basis thereafter.
5. The CHCN will foster and promote a culture of privacy at the clinic.

2. Procedures:

Training Clinical and Administrative Staff Members of Their Obligations

Step 1. Whoever hires a new staff member must tell The CHCN privacy officer that a new person has been hired.

Step 2. Before giving the person access to personal health information and every year after, The CHCN privacy officer or designate must:

2.1. Train the new staff member of his or her privacy obligations or require them to review an eLearning / video module;

2.2. Have the new staff member sign an agreement that:

2.2.1. S/he has received training;

2.2.2. S/he understands his or her privacy and security obligations; and

2.2.3. S/he is aware that not meeting the privacy and security obligations could lead to a disciplinary action including dismissal and reporting to legal authorities or professional bodies; and

2.3. Write in the *Training Log* that the staff member was trained and that the agreement was signed.

Step 3. The CHCN privacy committee will think of other ways in addition to training to foster and promote a culture of privacy.

Step 4. The CHCN must remove the staff member's access to medical records if the he or she fails to complete the training.

Before Accessing New Systems or Information

Step 1. If staff members need access to a new system or a new information repository, The CHCN privacy officer must:

1.1. Determine whether the new system or information repository requires new or different privacy and security messages than was provided during training;

1.2. Train the staff members on the additional privacy and security messages; and

1.3. Write in the *Training Log* that the staff member received additional training.

Contents of Training Materials

Step 1. The CHCN privacy officer or designate must create training materials relevant to the staff member's role.

Step 2. The training content may include the following messages if relevant to the staff member's role:

2.1. Defines personal health information and indicates that it is protected by PHIPA;

2.2. The CHCN is a health information custodian which means accountable for the information that it has on its clients;

2.3. Identifies why the staff member has access to PHI and specifically what he or she is allowed to do with it (i.e., purpose of collection, use, or disclosure);

2.4. Provides an overview of the privacy policies that are relevant;

2.5. What the staff member must do if a client has privacy questions or requests;

2.6. What the staff member must do to protect the PHI and privacy;

2.7. How to identify a Breach, what to do in the event of a Breach, and the consequences of a Breach; and

2.8. Anything the staff member needs to know about other shares systems.

Consent Management Policy and Operating Practice - PHIPA Reference: Sections 18-28

Templates or forms associated with these procedures:

- **Consent Directives Log**
- **Consent Directives Override Log**
- **Template of Messages to Discuss with client when Creating or Removing a Block**
- **Template of Messages to Discuss with client when an Override Occurs**

1. Policy:

1. The CHCN must obtain implied or express consent for collecting, using, and disclosing personal health information for healthcare purposes.
2. The CHCN must not collect, use, or disclose personal health information for healthcare purposes if the client wants it blocked (i.e., consent directives).
3. The CHCN must try to create a block that most closely matches the client's wishes. As an example, these may include:
   3.1. Block all or some of the medical record from being accessed by anyone or disclosed to another clinic for healthcare purposes;
   3.2. Block all or some of the medical record from being accessed by particular people in The CHCNor from being disclosed to named clinics; or
   3.3. Allow all or some members to access an otherwise blocked medical record.
4. The CHCN or an agent of The CHCN shall only override a client block to collect PHI where the agent or The Port Hope Northumberland Community Health Centre:
   4.1. Obtains the express consent of the client to whom the PHI relates;
   4.2. Believes on reasonable grounds that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to the client to whom the PHI relates and it is not reasonable possible to obtain the consent of the individual in a timely manner; or
   4.3. Believes on reasonable grounds that the collection is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the client to whom the PHI relates or to a group of persons.
5. When a staff member accesses personal health information that is blocked, The CHCN must confirm that it was appropriate and tell the client that blocked information was accessed.

2. Procedures:

Getting Consent

Step 1. The CHCN privacy officer must develop communications materials that are given to clients when they arrive at the clinic or that are posted in high-traffic areas.

Step 2. The communications materials must:

2.1. Contain a general description of the personal health information that The CHCN collects, uses, and discloses;

2.2. Describe what The CHCN does to protect either paper or electronic medical records;

2.3. Describe who at The CHCN has access to the medical records and why they have access;

2.4. Tell clients that they do not have to give consent to collect, use, or disclose for healthcare purposes and that they can block their medical record at any time (i.e., withdraw consent);

2.5. Inform clients that their personal health information is collected, used, and disclosed through shared electronic systems;

2.6. Give contact information for The CHCN privacy officer who can clients with their privacy-related issues and requests; and

2.7. Tell clients that they may make a complaint to the Information and Privacy Commissioner of Ontario and provide the contact information for the office.

Blocking the client Medical Record

Note: Blocking a medical record is a common term used when a client withholds or withdraws consent to collect, use, or disclose his or her medical record for healthcare purposes. This may also be known as a lockbox, consent withdrawal, consent directive, masking of the medical record, or various other names.

Step 1. If a client asks a staff member to create or remove a block on his or her medical record, the staff member must:

1.1. Discuss with the client the messages found in Template of Messages to Discuss when Creating or Removing a Block.

1.2. Help the client choose a block that most meets his or her needs (partial or total).

1.3. Put in a request to The CHCN privacy officer if unsure of how to Create or Remove a Block. Give the request to The CHCN privacy officer as soon as possible.

1.4. Verify the identity of the client by asking for photo identification or by asking another member of the clinic, if The staff member receiving the request is not known client

1.5. Confirm that the person is indeed the substitute decision maker for the client, if applicable, by following the Guidelines for Identifying a Substitute Decision Maker; and

When creating the block, The CHCN staff member must:

1.6. Create a block on the electronic medical record that most closely reflects the client's wishes (request help through IT department or Privacy Officer if needed)

1.7. Confirm with the client that the block was created or removed

1.8. Discuss with the client the messages found in *Template of Messages to Discuss with client when Creating* if this did not already happen;

1.9. Record in the chart that a request and block was made.

Blocking Medical Records in Shared Systems (i.e. Connecting Ontario, CHRIS HPG)

Step 1. The CHCN privacy officer must review the processes related to consent directives in shared systems to see whether there are any additional requirements that The CHCN must meet.

Step 2. If the client wants to create or remove a block in a shared system, The CHCN privacy officer must:

2.1. Follow the procedures laid out in the shared system agreement

2.2. Give the client contact information within 7 days for the program office responsible for the shared system (e.g., eHealth Ontario) if The CHCN cannot create the block for him or her.

Overriding client Blocks

Step 1. A staff member may only access personal health information that a client has blocked for one of the reasons outlined in Policy Statement #4 above.

When a staff member overrides a client block, The CHCN privacy officer must:

1.1. Follow-up with the staff member that overrode the block to make sure it was appropriate;

1.2. Discuss with the client the messages found in *Template of Messages when a Block Override Occurs;*

1.3. Provide the client with a hard copy of a letter that includes the messages above, unless the client says that you do not have to provide the letter; and

1.4. Follow the Privacy Breach Management Policy if the staff member overrode the block for an inappropriate reason.

After notifying the client of the override, The CHCN privacy officer must write in the *Consent Directive Override Log* that notice was made or keep a copy of the notice.

Logging and Auditing Policy and Procedure - PHIPA Reference: Sections 15. (3) (a), 17 (2)

Templates or forms associated with these procedures:

- **N/A**

1. Policy:

1. The CHCN will ensure that its internal systems log activities on the system where possible.
2. The CHCN will review its staff members to ensure that they comply with PHIPA, the privacy policies, and any agreements.

2. Procedures:

Logging Access and client Blocks

Step 1. Where possible, The CHCN must ensure that electronic systems containing client medical records record the following:

1.1. When information is viewed, accessed, or transferred to another system. The record should include:

1.1.1. client name or other identifiers;

1.1.2. client information that was handled;

1.1.3. Staff Member that handled the client information; and

1.1.4. Where the client information was transferred (if relevant); and

1.1.5. Date and time that the activity happened.

1.2. When client blocks are created, changed, or removed. The record should include:

1.2.1. client name or other identifiers;

1.2.2. Name of the person who requested the consent directive (i.e., the client or his or her substitute decision maker); and

1.2.3. Type of client block and the date and time that it was created, changed, or removed.

1.3. When client blocks are overridden. The record should include:

1.3.1. client name or other identifiers;

1.3.2. Staff Member who overrode the client block;

1.3.3. Type of client information that was viewed;

1.3.4. Reason for the override; and

1.3.5. Date and time that the override occurred.

Auditing Staff Members' Access to The CHCN's Systems

Step 1. The CHCN privacy officer must get audit reports on the access logs on a monthly basis.

Step 2. The CHCN privacy officer must choose an auditing approach[2].

Step 3. The CHCN privacy officer must provide the audit reports to the managers of the staff members being audited and ask them to confirm their staff members' access.

Step 4. The managers must follow-up with the staff members on any suspicious behavior that they identify.

Step 5. The managers must notify The CHCN privacy officer of any suspicious behavior for which the staff member is unable to provide a satisfactory explanation.

Step 6. The CHCN privacy officer must follow the breach management procedure for any unexplained, suspicious behavior.

Auditing Staff Members' Access to Shared Systems

Step 1. The CHCN privacy officer must follow the guidance provided by the relevant program office for auditing The CHCN's staff members' access to the shared system.

If no guidance is provided, The CHCN privacy officer will follow The CHCN's procedures for auditing staff members.

[2] See the *EHR Auditing and Monitoring Guide*, for suggestions implementing an audit program.

Retention Policy and Procedures - PHIPA Reference: Sections 13. (1), 13. (2)

Templates or forms associated with these procedures:

- **N/A**

1. Policy:

1. The CHCN will ensure records are protected and disposed of in accordance with the Information Security Policy.
2. The CHCN will retain records containing PHI for specified periods of time:
   2.1. Any information collected to respond to access and correction requests, inquiries, complaints, and information pertaining to consent directives must be retained for two years after the request was made.
   2.2. Any information created about a client as part of an investigation of Privacy Breaches and/or Security Incidents should be retained for two years after the Privacy Breach has been closed.
   2.3. Audit and monitoring reports that contain PHI created and maintained for compliance purposes should be retained for the longer of thirty years or when PHI is removed from the EHR.
   2.4. Information used for identity provider registration that contains PI should be retained for seven years after last use.
   2.5. System-level logs, tracking logs, reports and related documents for privacy and security tasks that do not contain PHI should be retained for a minimum of two years.
   2.6. Assurance-related documents should be retained for ten years.
   2.7. Where <<organization>> is an Identity Provider:
      2.7.1. Authentication events for sixty days online or twenty-four months total in archive; and
      2.7.2. End user credential information permanently.

Supporting Operating Practices

Identity Verification

Verifying client Identity

Step 1. If a staff member knows the client's identity and is able to confirm that the request is from that client, The CHCN privacy officer does not need to request identification.

Step 2. If a staff member does not know the client's identity, The CHCN privacy officer must request photo identification from the client. Valid forms of photo identification can be found in the *Identification Standards* attached to this operating practice.

Confirming that the Person is a Substitute Decision Maker for the client

Step 1. If a client brings another person to an appointment or says that a person is a substitute decision maker, the staff member does not need further proof that the person is a substitute decision maker.

Step 2. If the client is not able to tell the staff member that the person is a substitute decision maker, The CHCN privacy officer must request proof from the person that he or she is the substitute decision maker for the client. Valid forms of proof can be found in the *Identification Standards* attached to this operating practice.

Step 3. The staff member who confirms the authority of the SDM must tell The CHCN privacy officer of the relationship.

Step 4. The CHCN privacy officer must write the name of the substitute decision maker in the *SDM Log*.

Appendixes

Templates and tools can also be found at

G:\Policies and Procedures Manual\Organizational\Privacy\Forms Related to Privacy Compliance

Supporting Tools and Templates

Access and Correction

Request for Access Form

Request for Access Form - Template.doc

Instructions

Use the form attached to record requests: a client's request to view his or her medical record, or have the client complete it when making the request.

Copy and paste the template onto your letterhead. Customize the template to ensure it is appropriate for your clinic and replace the place holders (e.g., The CHCN privacy officer) with the appropriate information.

When the client makes the request: receive or complete the form, save it, and log it in *Request for Access Log*.

The completed form contains PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep the completed form for 2 years.

Request for Access Log

Instructions

1. Use this log to record when you receive a Request for Access and tracking status as you complete it.
2. Click on the icon for the Excel Worksheet to open the log template. Save it in an appropriate location.

3. The completed log may contain PI or PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep the completed form for 2 years.

Request for Access Response Template

Instructions

4. Use the appropriate letter template below for communicating with the client about the results of the request to obtain a copy of his or her medical record.
5. Copy and paste the letter template onto your letterhead. Customize the template to ensure it is appropriate for your clinic and replace the place holders (e.g., The CHCN privacy officer) with the appropriate information.
6. Complete the letter template and send it to the client within 30 days of receiving the request.
7. Save a copy of the completed letter or log the response in *Request for Access Log*.
8. The completed letter may contain PI or PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep the completed form for 2 years.

Use this template if you are releasing the entire medical record

Dear <<name of client>>,

This is a copy of your medical record. You asked for this information on <<date of request>>.

If you want to discuss this or have questions about what the information in your medical record means, please contact me at <<phone number for privacy contact>>.

Sincerely,

<<Name, Title>>

Use this template if you are not releasing all of the medical record

Dear <<name of client>>,

You asked for a copy of your medical record from our files.

We have decided not to give you a copy of <<any of/part of>> your medical record. This is allowed by Ontario law (Personal Health Information Protection Act, s52 (1) <<insert the number of the relevant clause in s52 (1)>>). We made this decision because <<provide reason that the access request is being denied as long as it does not expose the PHI being withheld>>.

<<If the request is being denied in part, briefly describe the nature of the medical records being withheld (e.g., mental medical records, medical records from a particular encounter, all medical records) if it does not expose the PHI being withheld, and whether some medical records are still being released.>>

If you want to discuss this or need more information, please contact me at <<phone number for privacy contact>>.

You also have a right under Ontario's laws to register a complaint about not getting access to your information. Contact the Information and Privacy Commissioner of Ontario to make a complaint:

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8

Telephone: (416) 326-3333 or (905) 326-3333
Toll free: 1 (800) 387-0073 (within Ontario)
TDD/TTY: (416) 325-7539
FAX: (416) 325-9195

Sincerely,

<<Name, Title>>

Use this template if you need more than 30 days to provide the person with the medical record

Dear <<name of individual>>,

We have received your request for a copy of your medical record. We will be able to provide you with the information however the retrieval of your information will take 30 days due to the following reason:

<<provide reason for the extension; note that the reason must be aligned with PHIPA, s54 (3) where it is a Request for Access or s55 (3) where it is a Request for Correction>>.

If you have any concerns or questions about why we need more time, please contact The CHCN privacy officer at:

The CHCN privacy officer
The Port Hope Northumberland Community Health Centre
<<HIC Address>>
<<HIC Phone>>
<<HIC Fax>>

Sincerely,

<<Name, Title>>

Request for Correction Form

Request for Correction Form Temp

Instructions

9. Use the form attached to record Requests for Correction to the client's medical record
10. Copy and paste the template onto your letterhead. Customize the template to ensure it is appropriate for your clinic and replace the place holders (e.g., The CHCN privacy officer) with the appropriate information.
11. When the client makes the request: receive or complete the form, save it, and log it in *Request for Correction Log*.
12. The completed form contains PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep the completed form for 2 years.

Request for Correction Log

Request for Correction Log Templ

Instructions

13. Use this log to record when you receive a Request for Correction and tracking status as you complete it.
14. Click on the icon for the Excel Worksheet to open the log template. Save it in an appropriate location.
15. The completed log may contain PI or PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep the log information for 2 years.

Request for Correction Response Template

Instructions

1. Use the appropriate letter template below for communicating with the client about the results of a Request for Correction.
2. Copy and paste the letter template onto your letterhead. Customize the template to ensure it is appropriate for your clinic and replace the place holders (e.g., The CHCN privacy officer) with the appropriate information.
3. Complete the letter template and send it to the client within 30 days of receiving the request.
4. Save a copy of the completed letter or log the response in *Request for Correction Log*.
5. The completed letter contains PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep the completed form for 2 years.

Use this template if you have made the correction

Dear <<name of client>>,

You asked that the following information about you be changed:

- **<<describe PHI that was inaccurate>>**

We made the following change:

- **<<describe the change that was made>>**

If you want to discuss this change, please contact me at <<phone number for privacy officer>>.

Sincerely,

<<Name, Title>>

Use this template if you are not making the correction

Dear <<name of client>>,

You asked that the following information about you be changed:

- **<<describe PHI that was inaccurate>>**

We decided not to make the changes because <<explain reason for not making the change which must be aligned with PHIPA, s55 (9).>>

If you want to discuss this or want to attach a note to your medical record saying that you do not agree with the information, please contact me at <<phone number for privacy contact>>.

You also have a right under Ontario's laws to register a complaint about our decision. To register your complaint, contact the Information and Privacy Commissioner of Ontario at:

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8

Telephone: (416) 326-3333 or (905) 326-3333
Toll free: 1 (800) 387-0073 (within Ontario)
TDD/TTY: (416) 325-7539
FAX: (416) 325-9195

Sincerely,

<<Name, Title>>

Use this template if you need more than 30 days to make the correction

Dear <<name of individual>>,

You asked us to make a change to your medical record.

We require an additional 30 days to investigate the change.

The additional time is required because <<provide reason for the extension; note that the reason must be aligned with PHIPA, s55 (3)>>.

If you have any concerns about the extra time, please contact The CHCN privacy officer at:

The CHCN privacy officer
The Port Hope Northumberland Community Health Centre
<<HIC Address>>
<<HIC Phone>>
<<HIC Fax>>

Sincerely,

<<Name, Title>>

Notice to HIC of a Correction to PHI Template

Notice to HIC of a Correction to PHI Ten

Instructions

1. Use the attached letter template for communicating with other HICs about the results of a Request for Correction that you have received, and that the patient has requested you notify any other HIC who has accessed his or her record.
2. Copy and paste the letter template onto your letterhead. Customize the template to ensure it is appropriate for your clinic and replace the place holders (e.g., The CHCN privacy officer) with the appropriate information.
3. Complete the letter template and send it to the relevant HIC(s).
4. Save a copy of the completed letter or log the response in *Request for Correction Log*.
5. The completed letter contains PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.

Inquiries and Complaints

Inquiry and Complaint Log

Inqiuiries and Complaints log.xlsx

Instructions

16. Use this log to record when you receive an Inquiry or Complaint, and to track how you manage and respond to it.
17. Click on the icon for the Excel Worksheet to open the log template. Save it in an appropriate location.
18. The completed log contain may contain PI or PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep the log information for 2 years.

Inquiry or Complaint Response Template

Instructions

19. Use this letter template to respond to a person making an Inquiry or Complaint.
20. The completed letter may contain PI or PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep the completed form for 2 years.

Template:

Dear <<name of individual>>,

We received a (Question/Complaint) from you on <<date of receipt>>.

<<Provide response here>>

If you have any other questions or concerns, please contact:

- **The CHCN privacy officer**
- **<<contact information for privacy officer >>**

(*Instruction: only include the following if it was a complaint*) **You can also contact Ontario's Information and Privacy Commissioner with privacy complaints. If you want to register a complaint, please contact:**

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario M4W 1A8

Telephone: (416) 326-3333 or (905) 326-3333
Toll free: 1 (800) 387-0073 (within Ontario)
TDD/TTY: (416) 325-7539
FAX: (416) 325-9195

Sincerely,

<<Name, title of privacy officer>>

Privacy Breach Management

Privacy Breach Log

Privacy Breach and Incident Log Templat

Instructions

21. Use this log to record privacy breaches, and to track how you manage and respond to it.
2. Click on the icon for the Excel Worksheet to open the log template. Save it in an appropriate location.
3. The completed log may contain PI or PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep the completed form for 2 years.

Privacy Breach Report

Privacy Breach Report Template.doc

Instructions

1. Use this report template to document a privacy breach. The report will be updated as the breach is contained, investigated, and remediated.
2. This form **must not contain personal health information**. Any personal health information which needs to be stored should be included as an appendix and must be removed unless the person receiving the report has authority and the need to view the information

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep the completed form for 2 years.

Training

Privacy eLearning Modules

eHealth Ontario makes a Connecting Ontario privacy eLearning module publicly available on its website. These modules include general privacy awareness in addition to processes that are specific to Connecting Ontario. Note that some of the processes are specific to Connecting Ontario and you may need to provide additional materials so that your staff members know the exact process that they need to follow for your organization.

Note: Training for privacy and security leads for Connecting Ontario will be provided by eHealth Ontario through scheduled live webinars hosted by eHealth Ontario.

Training Log

Privacy Training Log Template.xlsx

Instructions

22. Use this log to track when you provide privacy and security training to your staff members.
2. Click on the icon for the Excel Worksheet to open the log template. Save it in an appropriate location.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep the completed form for 2 years.

Consent Directives

Consent Directives Log

Consent Directives Log.xlsx

Instructions

23. Use this log to record when you make, modify, or remove a client block.
    24. Click on the icon for the Excel Worksheet to open the log template. Save it in an appropriate location.
    25. The completed log may contain PI or PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep information on this form for 2 years.

Request for Consent Directive Response Template

Notification of Consent Directive Ter

Instructions

1. Use the attached letter template for communicating with the client about the results of the request for a consent directive on his or her medical record.
2. Copy and paste the letter template onto your letterhead. Customize the template to ensure it is appropriate for your clinic and replace the place holders (e.g. The CHCN privacy officer) with the appropriate information.
3. Complete the letter template and send it to the client immediately after the consent directive has been implemented, modified or removed.
4. Save a copy of the completed letter or log the response in the Consent Directives Log.
5. The completed letter contains PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep information on this form for 2 years.

Notice of Consent Override

Consent Management - Templ

Instructions

1. Use the attached letter template for communicating with the client about the occurrence of a consent directive override.
2. Copy and paste the letter template onto your letterhead. Customize the template to ensure it is appropriate for your clinic and replace the place holders (e.g. The CHCN privacy officer) with the appropriate information.
3. Complete the letter template and send it to the client immediately after the consent override has been investigated.
4. Save a copy of the completed letter or log the response in the Consent Override Log.
5. The completed letter may contain PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.

Notice of Consent Override to IPC

Consent Management - Templ

Instructions

1. Use the attached letter template for notifying the Information and Privacy Commissioner of Ontario (IPC) about the occurrence of a consent directive override only if the override was performed for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person other than the individual to whom the PHI relates or to a group of persons.
2. Copy and paste the letter template onto your letterhead. Customize the template to ensure it is appropriate for your clinic and replace the place holders (e.g. The Port Hope Northumberland Community Health Centre) with the appropriate information.

3. Complete the letter template and send it to the IPC immediately after the consent override has been investigated.
4. Save a copy of the completed letter or log the response in the Consent Override Log.
5. The completed letter should not contain any PHI.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.

Consent Directives Override Log

Consent Override Log Template.xlsx

Instructions

26. Use this log to record when one of your staff members overrides a consent directive and that you notified the client.
    27. Click on the icon for the Excel Worksheet to open the log template. Save it in an appropriate location.
    28. The completed log may contain PI or PHI. Any copies must be appropriately protected against theft, loss and unauthorized use or disclosure as well as against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep information on this form for 2 years.

Template of Messages to Discuss with client when Creating or Removing a Block

Instructions

1. Use the appropriate template below to guide your discussion with clients when you create or remove a block from their medical records.
2. Write in the Consent Directives Log when you have had this discussion with the client or, if you are creating a letter based on this template, save a copy of the letter at <<location at clinic where the completed document is stored>>.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form if relevant should be stored in <<location at clinic where the completed document is stored>>.
3. Keep the completed form for 2 years.

Use These Messages when Creating a Block

When creating a block, talk to or write to the client about:

- The type of block that will be or was placed on the individual's file and how it will meet the client's request;
- The impact of a block on the client's care;
- When a consent directive can be overridden (3 purposes);
- That the client will be notified if the block is overridden;
- That the client can change his or her mind at any time, or create other blocks; and
- How to contact The CHCN privacy officer with any other questions or requests.

Use These Messages when Removing or Modifying a Block

When removing a block, talk to or write to the client about:

- Confirming that the block was removed or modified as requested;
- The type of block that was removed or modified and what information will now be made available;
- That the client can change his or her mind at any time, or create other blocks; and
- How to contact The CHCN privacy officer with any other questions or requests.

Template of Messages to Discuss with client when an Override Occurs

Instructions

1. Use the template below when discussing overrides with clients.
2. Write in the Consent Directives Override Log when you have had this discussion with the client or, if you are creating a letter based on this template, save a copy of the letter at <<location at clinic where the completed document is stored>>.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form if relevant should be stored in <<location at clinic where the completed document is stored>>.
3. Keep the completed form for 2 years.

Template

When a staff member overrides a client block, talk to or write to the client about:

- The type of client information that was viewed;
- The source of the client information (i.e., whether the information is from The CHCNor comes from another organization via a shared system);

- The staff member who overrode the block and the date / time that it was overridden;
- The reason that the block was overridden; and
- How to make a complaint to The CHCN privacy officer and Ontario's Information and Privacy Commissioner.

Note: there are three purposes for performing an override according to the *EHR Consent Management Policy*:

1. Patient has given express consent.
2. The HIC believes on reasonable grounds that the collection of PHI is necessary for the purpose of eliminating or reducing risk of serious bodily harm to the individual to whom the PHI relates, and it is not possible to obtain the consent of the individual.
3. The HIC believes on reasonable grounds that the collection of PHI is necessary for the purpose of eliminating or reducing risk of serious bodily harm to the individuals or a group other than the person to whom the PHI relates, and it is not possible to obtain the consent of the individual.

Identity Verification

Identity Verification Standards

Staff Members can rely on the following documentation of proof of identity. The Individual must present one of the following:

- Copy of ID issued by a federal, provincial/territorial/state or municipal authority and which bears a photo and signature of the Individual; or
- Copy of a student card bearing a photo and signature of the person, where the person is between 12 and 18 years of age, inclusively;
- Reliance on the parent or legal guardian's assertion of identity where the person is less than 12 years of age and where the parent or legal guardian's identity has been verified; or
- An assertion from eHealth Ontario or another organization trusted by CHCN of the person's identity.

The documents may be presented in-person, through mail, or by fax. Photocopies are acceptable.

Confirming Authority to Act as Substitute Decision Maker

Note that a staff member can rely on a client providing verbal confirmation that a person is his or her substitute decision maker.

Staff Members can rely on the following documentation of proof that the Individual making the request is the substitute decision maker for the client. The documents may be presented in-person, through mail, or by fax. Photocopies are acceptable.

client is under 12 years of age	• **A birth certificate for the client, signatures from both parents who appear on the birth certificate, and a photocopy of ID issued by a federal, provincial/territorial/state or municipal authority which bears a photo and signature of both parents;** • **A legal document demonstrating that the Individual has sole custody or guardianship for the client; or** • **An assertion from eHealth Ontario or another organization trusted by <<Name of organization>> of the person's identity.**
client is between 12 and 18 years of age, inclusively	• **A signed letter from the client and photocopy of ID issued by a federal, provincial/territorial/state or municipal authority or student card which bears signature of the client;** • **A legal document demonstrating guardianship or Power of Attorney; or** • **An assertion from eHealth Ontario or another organization trusted by <<Name of organization>> of the person's identity.**
client is above 18	• **A signed letter from the client and a photocopy of ID issued by a federal,**

	provincial/territorial/state or municipal authority which bears a photo and signature of the client • **A legal document demonstrating guardianship or Power of Attorney; or** • **An assertion from eHealth Ontario or another organization trusted by <<Name of organization>> of the person's identity.**
client is deceased	• **A letter signed by the client prior to his or her death and a photocopy of ID issued by a federal, provincial/territorial/state or municipal authority which bears a photo and signature of the client** • **A legal document demonstrating right to have access to the client's information; or** • **An assertion from eHealth Ontario or another organization trusted by <<Name of organization>> of the person's identity.**

SDM Log

SDM Log Template.xlsx

Instructions

29. Use this log to record when one of your clients has a substitute decision maker.

    30. Click on the icon for the Excel Worksheet to open the log template. Save it in an appropriate location.

    31. The completed form contains PHI. Any copies must be appropriately protected according to ensure that it is protected against theft, loss and unauthorized use or disclosure and to ensure that the information is protected against unauthorized copying, modification or disposal.

Document Storage and Handling Instructions

1. This template is stored in <<location at clinic where the template is stored>>.
2. The completed form should be stored in <<location at clinic where the completed document is stored>>.
3. Keep information on this form for 2 years after the person is no longer the client's SDM.

Glossary - The following terms are used in this policy manual:

Term	Meaning
Blocking a Record	• A client's withdrawing consent to collect, use, or disclose his or her health information for healthcare purposes • Also commonly known as a consent directive, withdrawal of consent, patient instruction, lockbox, or mask
Lock box	• A client's withdrawing consent to collect, use, or disclose his or her health information for healthcare purposes • Also commonly known as a consent directive, withdrawal of consent, patient instruction, block, or mask
Privacy Breach	• Any event where client information is collected, used, or disclosed counter to PHIPA, The CHCN's policies, or obligations defined in agreements binding The Port Hope Northumberland Community Health Centre. • Any event where a client's privacy rights under PHIPA, The CHCN's policies, or agreements binding The CHCNare breached.
Program Office	• The organization responsible for managing a shared system • eHealth Ontario is the Program Office for Connecting Ontario
Request for Access	• The right of a person to request a copy of or to see his or her medical record
Request for Correction	• The right of a person to request a correction to his or her health information if it is inaccurate or incomplete
SDM	• Substitute decision maker
Shared Systems	• Databases with medical records contributed by multiple clinics and viewable by multiple clinics • Example is Connecting Ontario, Integrated Assessment Record, and so forth
Substitute Decision Maker	• A person who has the authority to make a decision on an individual's behalf, including making Request for Access, Correction, consent directives, and so forth • Note that substitute decision maker is defined in PHIPA, 2004
Verify Identity	• The process of confirming that the person is who they say they are, and confirming their authority to act as substitute decision maker (if relevant)