INFORMATION TECHNOLOGY SERVICES

Privacy Office

Privacy Framework

INFORMATION TECHNOLOGY SERVICES

Privacy Policy

Information Technology Services (ITS) is a joint venture between
London Health Sciences Centre (LHSC) • St. Joseph's Health Care London (St. Joseph's)

Policy written by Anne McNaughton
Regional Privacy Consultant

Document Ownership

POLICY INFORMATION	
Policy Owners	Chief Privacy & Freedom of Information Officer (LHSC) Director, Privacy and Risk (St. Joseph's)
Policy Sponsors	IVP, Diagnostic Services & CIO VP, Patient Care & Risk Management
Policy Approvers	Chief Privacy & Freedom of Information Officer (LHSC) Director, Privacy and Risk (St. Joseph's)
Original Effective Date	February 7, 2017

Document Control

The electronic version of this document is recognized as the only valid version.

DOCUMENT IDENTIFIER AND LOCATION:	
Review Frequency:	This document will be reviewed at least once every two years.

Revision History

VERSION NO.	VERSION DATE	SUMMARY OF CHANGE	CHANGED BY
V.1	February 7, 2017	Original Document Creation	Anne McNaughton
V.2	December, 2019	Two Year Review Updates ▪ Update Privacy Deliverables ▪ Addition of Privacy Education & Confidentiality Agreement Policy ▪ Addition of Annual Attestation Process ▪ Minor formatting updates	Anne McNaughton

Table of Contents

1 PREAMBLE

1.1 PURPOSE

This Framework is designed to define the directives employed by London Health Sciences Centre (LHSC)/St. Joseph's Health Care London (St. Joseph's) acting as the Health Information Network Provider (HINP), to protect Personal Health Information (PHI) under its care and control.

- Ensure compliance with PHIPA and its Regulations with regards to "Service Provider" and "Health Information Network Provider" requirements.
- Define a framework and requirements for how the Privacy Services are managed.
- Extends, not replaces, HICs' existing privacy and security programs to connect them with the privacy and security programs of all the other organizations.
- Ensures that each HIC is meeting the same basic obligations and standards for privacy and security.
- Establishes mutual trust amongst the HICs that the others afford the same level of protection to PHI and Individuals that they themselves do.

1.2 DEFINITIONS

TERM	DEFINITION
Agent	As defined in PHIPA section 2.
Customer	Those parties who have entered into an agreement with LHSC/ St. Joseph's for the purpose of purchasing services.
Health Information Custodian (HIC)	As defined in PHIPA section 3(1).
Health Information Network Provider (HINP)	Meaning as set out in section 6(2) of the Regulation made under PHIPA, as being a person who provides services to two or more HICs where the services are provided primarily to HICs to enable them to use electronic means to disclose PHI to one another, whether or not the HINP is an agent of any of the HICs.
Originating HIC	Organization with custody and/or control over the PHI.
Personal Health Information (PHI)	As defined in PHIPA section 4(1).
Personal Health Information Protection Act, 2004 (PHIPA)	The Personal Health Information Protection Act, 2004, S.O. 2004, c.3, Schedule A
PHIPA Regulation	Ontario Regulation 329/04 made under PHIPA.
Privacy Breach	A privacy breach includes the collection, use or disclosure of PI/PHI that is not in compliance with applicable privacy law, or circumstances where PI/PHI is stolen lost or subject to unauthorized or inappropriate collection, use or disclosure, copying, modification, retention or disposal.
Service Provider	Meaning as set out in section 6(2) of the Regulation made under PHIPA. Synonymous with HINP.
Supplied (Shared) Services	Services provided by LHSC/St. Joseph's as HINP (as listed in section 1.3)

1.3 SUPPLIED SERVICES LISTING

DESCRIPTION	ACROYNM
Diagnostic Imaging Repository	SWODIN, DI-r
Picture Archiving and Communications System	PACS
Health Information System	Cerner, EPR
Emergency Neuro Imaging Transfer System	ENITS

1.4 SCOPE

1.4.1 In Scope

This Framework applies to all LHSC/St. Joseph's employees, affiliates, third party providers, operators and administrators of LHSC/St. Joseph's network and computing facilities including contractors and their respective agents, contractors and employees who use the Supplied Services or those that support the operation of these Supplied Services.

1.4.2 Out of Scope

This Framework does not replace any policies or procedure that individual Health Information Custodians may have in place at their own institutions.

1.5 REFERENCES

1.5.1 External Documents

- Personal Health Information Protection Act (PHIPA) 2004
- Personal Health Information Protection Act Ontario Regulation 329/04
- Canadian Standards Association, 1996, "*10 Fair Information Principles of the Canadian Standards Association's Model Code for the Protection of Personal Information* - CAN/CSA – Q830-96"
- Ontario Hospital Association, 2004, *"Hospital Privacy Toolkit: Guide to the Ontario Personal Health Information Protection Act."*

1.5.2 Information Technology Supplied Services Policies

SUBJECT	REFERENCE
Access or Correct PHI in HINP Control Policy	Section 5.1
Privacy Audits and Monitoring Policy	Section 5.2
Privacy Breach Management Policy	Section 5.3
Consent Management Policy	Section 5.4
Complaints or Inquiries Procedure	Section 2.9
Privacy Education & Confidentiality Agreements Policy	Section 5.5

1.5.3 Privacy Deliverables

Sites are required to have the following in place before being given access to any of our services:

REQUIREMENT	RATIONALE
Designated Privacy Officer	PHIPA Section 15(2), (3)
Written Public Statement that is available to the public as well as education material (brochures, posters, website, etc.)	PHIPA Section 16(1), 18(6) Principle 2: Identifying Purpose
Corporate plan for mandatory privacy education and training of staff, physicians, students, volunteers and contracted staff, as well as a strategy for ongoing privacy awareness reminders and updates.	PHIPA Section 15(3)(b) Principle 1: Accountability
Process for tracking completion of education/receipt of Privacy and Confidentiality Agreement.	Principle 1: Accountability
Develop template privacy wording for contracted agents/third parties who may have access to PHI - contracts, data sharing agreements, service agreements.	Sec. 17(1.1), (2)(iv)
Develop process to review relevant contracts, identify liabilities and revise to reflect Privacy responsibilities of contracted agents.	Principle 1: Accountability
Auditing (including process to audit individuals with high risk of breach, e.g. "VIPs")	PHIPA Section 12(1)
Breach Management process which includes instructions for notifying a professional college in the event of a confirmed privacy breach.	Sec. 17.1 (2-5) O. Reg. 329/04, s.6.3 (1, 1-5)
Privacy policy which outlines the general framework of your organization's privacy program.	Sec. 10 Principle 8: Openness
Confidentiality policy which defines what is considered Confidential Information and the protections in place to maintain it.	Sec. 10
Identity and Access Control policy or standard which outlines the controls used to manage access to PHI.	Sec. 11.1, 17(1)(b)
Security of Confidential Information & Information Technology Systems policy which outlines the IT controls in place to safeguard PHI/CI and who is responsible for ensuring its enforcement.	Sec. 12(1)
Remote Access policy which describes how PHI/CI should be handled when using non-IT supplied resources.	Sec. 12(1)
Observer/Vendor Representative policy outlining which types of PHI the observer may have access to.	Sec. 12(1)
Breach of Privacy policy which defines a privacy breach and guidelines for managing the breach.	Sec. 12(2), 16(2)
Records Retention and Disposal policy which outlines how records under the custody and control of the HIC are to be stored and/or disposed of.	Sec. 13(1)
Retention Schedule which outlines how long PHI is to be kept for.	Sec. 13(2)
Access to PHI policy which outlines the process for allowing access to PHI in the custody and control of the HIC.	Sec. 52(1)

REQUIREMENT	RATIONALE
Disclosure of PHI policy which outlines the process related to disclosures of various types (bodily harm, law enforcement, proceedings, research, prescribed entities, other Acts, etc.).	Sec. 38-50
Correction of PHI policy which outlines the steps required to make a correction request by an individual.	Sec. 55(1-13)
Consent Directives policy.	Sec. 19(1)(2), 38(3)
Use of PHI for Research, Education, Quality Assurance and Risk Management policy.	Sec. 44(1-6), 37(1)(c-j), 37(3)
Process to support an individual's request to view or obtain a copy of the health record (Release of Information).	Sec. 11(2)
Breach Management process which outlines the steps to take should a privacy breach occur.	Sec. 12(2), 16(2)
Designated person and process for managing privacy audits provided by the HINP.	Sec. 12(1)
Requirement that all portable devices that may contain PHI/CI be encrypted.	Sec. 12(1)
Method of transferring PHI/CI securely to 3rd parties such as secure file transfer or FTP.	Sec. 10(1), 12(1)
If a 3rd party document destruction company is employed by your organization, is there an agreement in place that safeguards PHI?	Sec. 13
Substitute Decision Maker (SDM) identification process in cases where the individual is deemed incapable.	Sec. 22(3)
Process for verifying an individual's identity when an access or disclosure is requested.	Sec. 54(9)
Guidelines about what types of information can be disclosed about an individual to another individual whether in-person or via telephone (i.e. family or friends).	Sec. 38(3)
Process to document when an override of a consent directive has occurred to eliminate or reduce a significant risk of serious bodily harm.	Sec. 40(2)
Process for handling complaints which includes a direction to contact the IPC if the individual choses to do so.	Sec. 54(8)
Process to identify users who no longer need access to the system or when their privileges change.	Sec. 11.1
Process in place to log all inappropriate collections, uses, disclosures so they can be reported to the IPC on or before the March deadline each year.	O. Reg. 329/04, s. 6.4 (1)(2)
Process for addressing requests from patients to restrict access, use and disclosure of PHI (i.e. lockbox, anonymous status, Denial of Access, etc.).	Sec. 19 (1)(2), 38 (1)(3)
Document/brochure that explains the consent directives process and the risks associated with restricting access to the patient record.	Sec. 18 (6), 21 (1)(b)
Consent directives process which includes instructions for applying these restrictions in other external systems (eHealth applications, eCHN, etc.).	Best Practice Decision 102
Policy or procedure to allow patients to restrict collection, use, or disclosure of their PHI for fundraising purposes.	Sec. 32(1)

REQUIREMENT	RATIONALE
Process for managing consent when an individual requests to withhold/withdraw religious affiliation information.	Sec. 20(4)

1.5.4 Annual Attestation Process

After the initial determination of compliance with the Privacy Deliverables, all participating sites complete a checklist on an annual basis confirming that they are in compliance with current privacy legislation and IPC best practice guidelines.

The results of the annual attestation are distributed to all participants in the shared system(s) as confirmation of a minimum standard of compliance with respect to each individual HIC's information practices.

As an administrative safeguard, this ensures mutual accountability.

2 PRIVACY PRINCIPLES

This privacy policy has been designed to reflect the 10 Fair Information Principles contained in the Canadian Standards Association's *Model Code for Protection of Personal Information* as it is recognized as a national standard for privacy protection and the basis for PHIPA legislation.

2.1 ACCOUNTABILITY

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

LHSC/St. Joseph's is committed to ensuring the highest standard of privacy and data protection as applied in the services and technologies it manages.

The Privacy Program is jointly overseen by the Chief Privacy Officers of both London Health Sciences Centre and St. Joseph's Health Care London. They are responsible, in conjunction with the Regional Privacy Consultant, for implementing and maintaining the Information Technology Services privacy program which ensures compliance with applicable privacy legislation.

Key components of the Information Technology Services privacy program include:

- A collection of privacy policies and procedures which support the effective management and operationalization of privacy by the HINP.
- An extensive privacy-based training program for staff and affiliates.
- Privacy and Security assessments of all Supplied Services which involve PHI.
- Procuring Agreements which formally establish roles and responsibilities related to management and protection of PHI.
- Ensuring all participating and contributing HICs are compliant with the Privacy Deliverables (1.5.3).
- A governance committee for metric reporting and accountability.
- Monitoring of all HINP staff and affiliates with access to PHI, to measure, assess and report compliance with its privacy policies and standards.

2.2 PURPOSE OF COLLECTION

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

LHSC/St. Joseph's does not collect or disclose PHI while providing services to HICs, unless explicitly authorized by a HIC to act as an agent of the HIC.

Participating HICs are responsible for making the purposes for which PHI is collected, used and disclosed known to the patient at or prior to time of collection.

HICs are responsible to ensure they have the appropriate legislative authority to collect PHI while using any of the Supplied Services.

2.3 CONSENT

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

HICs are responsible for complying with knowledge and consent requirements, which require that individuals be made aware of the purposes for which their data is being collected, used and disclosed.

The individual has the right to establish a consent directive on their PHI at any time. A consent directive is an express instruction of an individual to their HIC regarding use or disclosure of their PHI.

HINP may implement consent directives for the Supplied Services at the request of the HIC (for instances when the HIC is not able to apply the consent directives themselves) by following the procedure detailed in Section 5.4 and completing Appendix F –Consent Management Form – "Lockbox".

2.4 LIMITING COLLECTION

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

LHSC/St. Joseph's will not collect or disclose PHI while providing services to HICs unless explicitly authorized for the purpose of providing services to the HIC. LHSC/St. Joseph's is permitted to receive only the information that is shared by the HIC.

2.5 LIMITING USE, DISCLOSURE AND RETENTION

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

2.5.1 LHSC/St. Joseph's Use of PHI

LHSC/St. Joseph's will only use PHI for providing services to HICs according to its contractual obligations and only for provision of health care, the assistance in provision of health care and/or with written approval of the HIC.

2.5.2 LHSC/St. Joseph's Disclosure of PHI

LHSC/St. Joseph's will not disclose any PHI to third parties except with express consent of HICs, for system troubleshooting and maintenance or as required by law.

2.5.3 LHSC/St. Joseph's Retention of PHI

LHSC/St. Joseph's will document Retention Schedule for PHI that is stored in its systems.

2.5.4 Access Control

Access controls are used to prevent unauthorized or inappropriate access to PHI, ensure protection of LHSC/St. Joseph's Supplied Services systems, prevent unauthorized computer access, detect unauthorized or inappropriate activities and ensure information security.

LHSC/St. Joseph's only grants PHI access to authorized persons based on roles and responsibilities for each position within the organization and only to the extent they require to fulfill the requirements of their job.

HICs are expected to adhere to similar principles based on their corporate policies and procedures and as outlined in the Purchased Service Agreement with reference to the Privacy Deliverables (Section 1.5.3).

2.5.5 Access Logging

LHSC/St. Joseph's keep an electronic record of accesses to all or part of the PHI contained in their Supplied Services and ensures the record identifies the person who accessed the information and the date and time of the access at minimum.

LHSC/St. Joseph's makes available to a HIC, as per the Information Technology Services Auditing Schedule, or upon request, logging reports regarding access to PHI that is in the HICs custody and control.

Each HIC is responsible for determining the validity of the access by its authorized users. An authorized person is one who requires access to PHI as part of their duties and understands their responsibilities to protect the confidentiality of the PHI.

2.5.6 Access by Third Party Service Providers

LHSC/St. Joseph's will use contractual or other means to ensure that a comparable level of protection is applied to restricting use, transfer and retention of PHI by retained third party service providers. These obligations may include signing of confidentiality agreements, participating in Privacy and Confidentiality training, explicit approval for remote access, etc.

2.6 ACCURACY

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

The accuracy of PHI is the responsibility of the HIC who collects it. Any corrections or changes to PHI must be completed by the HIC who has custody and/or control of the PHI.

LHSC/St. Joseph's will assist in the correction of individual records when informed of inaccuracies by participating HICs.

LHSC/St. Joseph's, where possible, provides mechanisms to HICs to support the accurate entry of PHI into the Supplied Services. LHSC/St. Joseph's also maintains, through its information security practices, mechanisms to protect the integrity of the PHI (see section 2.7 below).

2.7 SAFEGUARDS

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

2.7.1 Security Safeguards

LHSC/St. Joseph's implements administrative, technical and physical safeguards to protect PHI from unauthorized access, disclosure, copying, use, modification, loss or destruction, regardless of format and media in which it is stored. These safeguards are listed in detail in the *Security of Confidential Information and Information Technology Systems* policy which can be provided upon request.

2.7.2 Compliance Monitoring

LHSC/St. Joseph's provides mechanisms and services to HICs to assist them in meeting their obligations to comply with PHIPA. Specifically, LHSC/St. Joseph's executes a systematic and transparent set of monitoring processes including but not limited to the following:

- Program to track key dimensions of PHI handling, including:
    - Audit logging of all accesses to PHI
    - Compliance with Privacy Deliverables (section 1.5.3)
- Business process monitoring, including maintaining up-to-date policies and procedures, metrics regarding audit and breach management.

2.7.3 Privacy Impact Assessments

A Privacy Impact Assessment (PIA) assesses and identifies privacy risk and the level of privacy compliance with LHSC/St. Joseph's policy and legal requirements for an identified program or system. LHSC/St. Joseph's (or a designated third party) completes a PIA where significant changes are made that may pose risk or impact privacy compliance.

LHSC/St. Joseph's will provide a summary of the outcome of the PIA to the Health Information Custodians upon request.

2.7.4 Threat and Risk Assessments

A Threat and Risk Assessment of the Supplied Services identifies the risks associated with the confidentiality, integrity and availability of all data, including PHI which is managed and maintained on the Supplied Services systems. LHSC/St. Joseph's conduct TRAs where significant changes are made that may pose risk or impact privacy compliance.

LHSC/St. Joseph's will provide a summary of the outcome of the TRA to the Health Information Custodians upon request.

2.8 OPENNESS

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

LHSC/St. Joseph's has a legislative responsibility to be open and transparent about how it manages and protects PHI, and to inform individuals of their privacy rights (PHIPA s.3 (2), (3)).

LHSC/St. Joseph's makes available to HICs and the public:

- A plain language discussion of PHIPA and its regulations which apply to the Supplied Services;
- LHSC/St. Joseph's roles and obligations under PHIPA and its regulations;
- Summaries of results of PIAs where required.

LHSC/St. Joseph's will facilitate interaction between patient and HIC if individual is requesting information regarding the Supplied Services or how their PHI relates to the Supplied Services.

2.9 INDIVIDUAL ACCESS

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Under PHIPA, an individual has the right to access a record of their PHI that is in the custody or under the control of a HIC. In response to a written request for access, the HIC is required to either grant the request and provide access, or deny access based on a set of exemptions set out in PHIPA. Individuals also have the right to ask the HIC to correct any inaccurate or incomplete information.

Under the provisions of PHIPA, LHSC/St. Joseph's, acting as HINP, are not responsible for individual requests to access or correct PHI. If LHSC/St. Joseph's receives an access or correction request, it shall direct the individual to the appropriate HIC(s) to respond to the request.

2.10 CHALLENGING COMPLIANCE

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

Any person may submit a complaint and/or feedback (including inquires, compliments and suggestions) related to:

- LHSC/St. Joseph's privacy and data protection practices;
- LHSC/St. Joseph's information management practices; or

- Non-compliance with LHSC/St. Joseph's policies, or statutory or regulatory requirements.

Complaints and/or other feedback with respect to HINP services may be submitted using the following LHSC/St. Joseph's contact information:

Privacy Office
800 Commissioners Road, E. Building 24, LL-115
London, ON N6A 5W9
Fax: 519-667-6706
Phone: 519-685-8500 x.77992
Email: regionalprivacy@lhsc.on.ca

PHI should not be submitted with the description of the complaint or other feedback; however, LHSC/St. Joseph's may request this level of detail during the course of its investigation. LHSC/St. Joseph's acknowledges receipt of a complaint and/or other feedback within five business days of the receipt. Response regarding the outcome of the investigation will occur within 30 business days. If this timeframe cannot be accommodated, the individual shall be notified with the approximate time frame until a response occurs.

Complaints regarding a HIC will be directed to the appropriate individuals at that organization. If the complaint could have an influence on agreements or compliance monitoring, LHSC/St. Joseph's may choose to follow up on the investigation.

Individuals may file a complaint with the Information and Privacy Commissioner of Ontario (IPC) if any of the following have occurred:

- They feel they have incorrectly been denied access to their PHI;
- A HIC refused to make a requested correction to their PHI;
- More than 30 days has passed since the access or correction request was made, and the individual has not received a decision;
- The feel the HIC's estimate of fees is excessive.

All complains to the IPC must be in writing or be submitted though the form available on the IPC's website: https://www.ipc.on.ca/wp-content/uploads/Resources/cmpfrm-e.pdf

3 REGULATORY OBLIGATIONS

PHIPA establishes a statutory privacy framework for protecting PHI. The PHIPA Regulation also specifies requirements for providers to custodians that enable HICs to use electronic means to collect, use, modify, disclose, retain or dispose of PHI. The PHIPA Regulation further specifies requirements for HINPs that enable two or more HICs to use electronic means to share PHI.

3.1 PROVIDER REQUIREMENTS

LHSC/St. Joseph's will restrict the use, disclosure and retention as specified in Section 2.5 of this Framework in compliance with s.6(1) of PHIPA Regulation while providing services to enable HICs to use electronic means to collect, use, modify, disclose, retain or dispose of PHI.

3.2 HINP REQUIREMENTS

3.2.1 Breach Notification

HINP will notify every applicable HIC at the first reasonable opportunity of any privacy breach, suspected privacy breach or privacy risk related to the unauthorized access, use, disclosure, or disposal of PHI managed by LHSC/St. Joseph's or its third party service provider (s.6(3) (1), PHIPA Regulation).

The Information Technology Services Breach Management Protocol will be followed in the event of a breach as a result of any unauthorized event listed above.

Related Documentation: Privacy Breach Management Protocol (section 5.3)

3.2.2 Plain Language Description of Services and Safeguards

HINP will provide each participating HIC with a plain language description of the service provided and safeguards that have been implemented to protect PHI against unauthorized use or disclosure, and to protect the integrity of the information (s. 6(3) (2), PHIPA Regulation).

HINP will ensure that the following information is provided to each participating HIC:

- Description of service provided in service agreements with participating HICs.
- Description of the administrative, technological and physical safeguards in place to protect PHI.
- The contact information for the Information Technology Services Privacy Office.

Related Documentation: Appendix A - Plain Language Description

3.2.3 Public Description of Services, Safeguards, Directives, Guidelines and Policies

HINP will make available to the public a plain language description of services provided and the safeguards employed to keep PHI secure and confidential. This public description will include any directives, guidelines and policies that apply to these services (PHIPA Regulation, s. 6(3) (3)).

HINP will ensure that the following are available to the public and key stakeholders:

- Description of services provided.
- Description of the administrative, technical and physical safeguards in place to protect PHI.
- The contact information for the Information Technology Services Privacy Office.

Related Documentation: Appendix A – Plain Language Description

3.2.4 Provision of Audit Logs

HINP shall to the extent reasonably practical, and in a manner that is reasonably practical, keep and make available to each HIC, an electronic record of all accesses and transfers of PHI associated with the HIC (s.6 (3) (4), PHIPA Regulation).

HINP has established an Information Technology Services privacy audit policy to comply with PHIPA.

Related Documentation: Privacy Auditing Policy (section 5.2)

3.2.5 Providing HICs with a Privacy Impact Assessment and Threat Risk Assessment of Services Provided

HINP shall perform and provide each participating HIC a written copy of the results of an assessment of the Privacy Impact and Threat Risk Assessment on the services provided (s.6 (3) (5), PHIPA Regulation).

HINP will conduct privacy impact assessments (PIAs) and threat risk assessments (TRAs) on all new or significantly amended services provided by LHSC/St. Joseph's as HINP. The key findings and recommendations of conducted PIAs and TRAs will be shared with the participating HICs upon request.

Due to the sensitive nature of these documents, they will be provided to the HIC's Privacy or Security Officer.

3.2.6 Restrictions on Employees and Third Parties

HINP will ensure that all employees or third parties retained to perform services comply with LHSC/St. Joseph's privacy and security restrictions and conditions (PHIPA Regulation s.6 (3) (7)).

The use of PHI for the provision of services will be restricted to LHSC/St. Joseph's staff (including third-parties) who require access in order to perform those services. To obtain access, staff will be required to:

- Sign a privacy and confidentiality agreement.
- Successfully complete privacy training on an annual basis.

Third-party service providers will be required to sign an Agreement which assures the protection of PHI.

Related Documentation: Appendix B - Sample Privacy & Confidentiality Form

3.2.7 Written Agreement with Respect to Services and Safeguards

HINP will enter into a written user agreement with each participating HIC describing the services provided, the administrative, technical and physical safeguards in place to protect the confidentiality and security of the information, and that requires LHSC/St. Joseph's to comply with PHIPA and its Regulations (s.6 (3) (7), PHIPA Regulations).

HINP will ensure that the agreements with HICs include the following restrictions:

- HINP will not use PHI to which it has access in the course of providing services except as necessary in the course of providing these services.
- HINP will not disclose PHI to which is has access in the course of providing services.
- All HINP employees and third parties agree to comply with LHSC/St. Joseph's privacy and security requirements.

4 ROLES AND RESPONSIBILITIES

4.1 INFORMATION TECHNOLOGY PRIVACY RESOURCES

- Provide advice and guidance to the Privacy Officers of participating organizations on privacy-related issues.
- Act as a conduit between London Privacy Resources and the Privacy Officers of participating organizations.
- Assist the Privacy Officers of participating organizations with privacy-related policy development and privacy education material.
- Provide recommendations to the organization to assist in minimizing their privacy risk.
- In collaboration with London Privacy Resources, conduct privacy reviews on initiatives related to Personal Health Information that would impact the region.
- Chair the Information Technology Services Privacy Committee meeting on a quarterly basis.
- Review the Privacy Deliverables compliance list with the Privacy Officers of participating organizations.
- Ensure privacy compliance as per the Master Purchased Services Agreement in keeping with our role as the HINP.
- Provide random, requested and trigger auditing reports of all Supplied Services as per auditing schedule.
- Communicate suspect privacy breaches to Privacy Officers of participating organizations.
- Counsel, advise and educate the interpretation of the audits.
- Complete the Organization's Auditing Tracking Flowsheet for each audit performed.
- Supply the Auditing Tracking Flowsheet and Summary Report upon completion of each audit.
- Maintain auditing statistics for Privacy Scorecard reporting on a quarterly basis.

4.2 PARTICIPATING HICs

- 100% compliance with privacy deliverables.
- Complete privacy investigation on privacy audit reports provided as required.
- Report Privacy Audit Flowsheet statistics in a two week turnaround timeframe.
- Provide ongoing privacy education to staff and affiliates.
- Attend Information Technology Services, Privacy Committee Meetings.

5 POLICIES AND PROCEDURES OVERVIEW

5.1 ACCESS OR CORRECT PHI IN HINP CONTROL

Summary

The purpose of this policy is to define the policies and procedures that apply in receiving and responding to access and correction requests with respect to the Supplied Services made by the Individual to whom the PHI relates. The key principles of the policy are:

If a HIC receives an access or correction request:

- If the request relates to PHI that was contributed or collected (i.e., viewed) by someone at your organization: respond to the request.
- If the request relates to PHI that was contributed by another HIC: ask the person to contact the HIC that contributed the PHI to make the request.
- If the request relates to PHI that was contributed by more than one other HIC: ask the person to contact HINP.

If the HINP receives an access or correction request:

- If the request relates to PHI that was contributed by one HIC: HINP will ask the person to contact the HIC that contributed the PHI to make the request.
- If the request relates to PHI that was contributed by more than one HIC: HINP will forward the request to the HIC(s) that contributed the PHI, coordinate the response and perform all the administrative functions
- If the request relates to PHI that was contributed by one or more HICs but cannot be corrected at the source: HINP will perform the correction after receiving the Correction/Amendment of PHI form from the applicable HIC.

Required Forms

Appendix C - Correction/Amendment of PHI Form

5.2 PRIVACY AUDITS AND MONITORING

Summary

The purpose of this policy is to define the policies and procedures that apply in logging, auditing, and monitoring viewing, handling, and dealing with PHI within the Supplied Services.

General Audit Information

- All audits run (scheduled or requested) must be documented on the Audit Flowsheet, regardless of whether the audit report does or does not show any accesses. This information is provided to each HIC's Privacy Officer quarterly in preparation for reporting to the governance committees.
- All audits are provided to the HIC's Privacy Officer via Secure File Transfer.
- Final clearance of user accesses/activity in any shared system is the responsibility of the HIC. As the HINP, we may be contacted to provide additional information or assistance with interpreting the audit, but it is out of scope of our duties to clear any accesses.

Scheduled Audits

5.2.1 Random User Audit

User is selected using a Random Number Generator (RNG) (https://www.random.org/) based on each HIC's active user list. The list is filtered to show only those users who have accessed any of the Supplied Services in the previous month. The total of active users in this list is the number used in the "Max" box of the random number generator. The number generated using this tool now corresponds to the row number in the excel file of the user who is to be audited. Ex. the number of active users within the last month on the excel file is 100. The number 100 is then used as the Max in the RNG tool. After clicking on "Generate", a result of "65" is displayed and that number is now the row number used to choose the person who is to be audited.

Each audit is run for a period of two weeks based on the agreed upon schedule distributed at the beginning of each new fiscal year.

5.2.2 Same Last Name Audit (SLNA)

The SLNA report is run for a two week period, with frequency based on the agreed upon schedule. This audit will show results if a person has accessed any of the Supplied Services using the same last name as what the user is registered under. It will detect whether they have looked at their own record or others with the same last name.

Requested Audits

Health Information Custodians may request audits using the Supplied Services Audit Request Form. HICs must complete the audit request form and fax it to the dedicated fax line in the LHSC Privacy Office or send it via Secure File Transfer to regionalprivacy@lhsc.on.ca.

Requested Audits will be run as a priority to normal scheduled audits unless the HIC has indicated otherwise.

SWODIN Repository to Confirm ClinicalConnect Image Viewing

Audits on the SWODIN Repository are part of the audit investigation process for organizations that use the SWODIN/ClinicalConnect interface. The ClinicalConnect audit report (retrieved by requesting an audit via ClinicalConnect support) must show that the user launched the SWODIN viewer window via ClinicalConnect to trigger a request for an audit of the SWODIN repository. The SWODIN Repository will show the accession and date/time of the access only.

To request an audit of the SWODIN Repository once access is confirmed, complete and return the Supplied Services Auditing Request Form.

Required Forms

Appendix D - Audit Request Form

5.3 PRIVACY BREACH MANAGEMENT

Summary

The purpose of this policy is to define the policies and procedures that apply in identifying, reporting, containing, notifying, investigating, and remediating privacy breaches with respect to the shared services. The key principles of the policy are:

- All breaches involving multiple organizations in any of the shared services must be reported to LHSC/St. Joseph's.
- All impacted HICs will be notified of the breach.
- The Regional Breach Management Protocol will be followed.

Identifying a Privacy Breach

A privacy breach occurs when a health information custodian or agents acting on their behalf:

- have contravened a provision of the Personal Health Information Protection Act, 2004 (PHIPA) or the PHIPA Regulation;
- believes or has reason to believe that personal health information involved within the services has been lost, stolen, or has been used, accessed, disclosed, copied, modified or destroyed in an unauthorized manner;
- collects, uses or discloses personal health information for purposes other than those described in the Purchased Services Agreement or Service Agreement (ENITS);
- contravenes the applicable privacy provisions of the Purchased Services Agreement or Service Agreement (ENITS).

A multi-org. privacy breach occurs when PHI for one or more patients is lost, stolen or has been used, accessed, disclosed, copied, modified or destroyed in an unauthorized manner by an agent of a Receiving HIC.

A multi-org breach may also occur if the HINP is responsible for the loss, or unauthorized use, access, disclosure, copy, modification or destruction of PHI for which it is not the HIC.

Managing and Reporting a Multi-Org Privacy Breach

If a breach occurs that affects more than one HIC, the investigation, containment, remediation and notification must be a coordinated effort while respecting the individual corporate privacy breach policies and procedures.

The Regional Privacy Consultant must be notified in writing and within 1 business day of confirming a multi-org breach has occurred. The Regional Privacy Consultant may be brought in to assist in coordinating the process. HICs must agree to the following:

- The Lead Organization is identified as the HIC whose agent was the cause of the breach, though all HICs impacted are expected to assist in the process as required. The Lead Organization will have a greater interest in the incident and will be responsible for:
    1. Leading the breach management process;
    2. Notifying the individual(s) to whom the PHI relates*;
    3. Notifying the IPC of the breach if applicable; and

4. Notifying other parties as applicable including any provincial assets (e.g. OLIS) or other shared information systems (e.g. ClinicalConnect).

*If the patient is unable to be notified (e.g. patient is deceased or having no fixed address), the Lead Organization will ensure that an attempt to notify the Substitute Decision Maker is done, and if this is unsuccessful, a copy of the notification will be placed on the patient's chart. The notification should be placed on the chart at the HIC where the breached PHI was collected and where the patient receives the most frequent care so notification can be done at a future visit (if applicable).

Multi-Org Breach by the HINP

If PHI is lost, stolen or inappropriately accessed by the HINP and the HINP is not the HIC of the affected PHI, the HINP will notify the affected Customers in writing within 1 business day of confirming that a multi-org breach occurred.

The HINP, through the Regional Privacy Consultant, will provide a written report to the affected Customers once the investigation is complete and may be required to provide a report to the appropriate governance body(ies) regarding the incident. The report will include:

- A description of the privacy breach;
- The circumstances under which the privacy breach occurred; and
- The steps the HINP is taking to address the breach and minimize the risk of recurrence.

Other parties outside of the Purchased Services Agreement or Service Agreement (ENITS) may need to be notified (i.e. eHealth Ontario, Information and Privacy Commissioner, LHIN representatives, MOHLTC). Notification of these external parties will be managed per any contractual agreements or legislative obligations between the HINP, the affected HIC(s) and the external party.

5.4 CONSENT MANAGEMENT

Summary

The purpose of this policy is to define the policies and procedures that apply in obtaining the consent of the Individual in respect of the collection, use or disclosure of the Individual's PHI in any and/or all of the Supplied Services (where applicable), and that apply in making, modifying, withdrawing, or overriding consent directives in respect to PHI hosted by the Supplied Services. The key principles of the policy are:

Obtaining Consent:

- HICs follow their existing policies and procedures regarding their approach to consent.
- Provide patient with a brochure or document regarding consent directives if they request more information.

Managing Consent Directives:

- If technical ability exists, consent directives should be applied, modified, or deleted by the HIC. In cases where this is not possible, HIC should contact the Regional Privacy Office to facilitate the consent directive using the Consent Management Form.
- It is the requesting HICs responsibility to provide notice to patient when the request is completed.

How Lockbox Affects All Participants in the Shared Systems:

- Once a consent directive is placed on a patient's chart in any of the shared systems, it is applicable to all sites who participate. Applying a lockbox is a "global" setting for all of our shared systems.
- PHIPA section 38(2) requires that a disclosing custodian notify all parties to the disclosure that there is restriction placed on that patient's PHI and that not all information is available.
    - Due to a technical inability to do this in an efficient manner, the term "lockbox" is placed in the middle name field of all patients with lockbox provisions. This is the signal to all participants that a consent directive has been applied.

Required Forms

Appendix F - Consent Management Form

5.5 PRIVACY EDUCATION & CONFIDENTIALTY AGREEMENTS

Summary

The purpose of this policy is to define the privacy education and confidentiality agreement standards that apply to all participants in the shared systems. The expectation is that all participants are compliant with the guidelines given by the Information and Privacy Commissioner of Ontario regarding privacy education and signing of confidentiality agreements. These two standards are combined as they often are completed concurrently in electronic training systems. The key principles of the policy are:

Privacy Education and Training:

- HICs are autonomous in creating the content for their privacy education and training.
- IPC guidelines suggest that privacy-related education materials be available to all agents (e.g. newsletters, pamphlets)
- IPC guidelines state that privacy education and training should be completed by agents who have access to personal health information upon hire and on an annual basis thereafter.
- Privacy training and education should be completed by all 3rd parties prior to accessing any system containing personal health information.
- Privacy training and education completion should be tracked and available for verification at a later point in time.

Confidentiality Agreements:

- HICs are autonomous in creating the language for their confidentiality agreements.
- In addition to privacy training and education, IPC guidelines state that all agents are required to sign a confidentiality agreement upon hire and annually thereafter. This can be documented on paper or electronically.
- All 3rd parties are required to sign confidentiality agreements prior to accessing any system containing personal health information.
- Confidentiality agreement completion should be tracked and available for verification at a later point in time.

Annual Attestation Process:

- As described in section 1.5.4 Annual Attestation Process, it is up to each HIC to ensure that they are following all the legislated requirements and IPC guidelines for their respective privacy programs. As a safeguard to all sites participating in the shared services, an annual attestation process occurs.

Required Forms

Appendix B - Sample Privacy & Confidentiality Form

Appendix G - Annual Privacy Program Attestation

6 APPENDICES

Appendix A Plain Language Description

Appendix B Sample Privacy & Confidentiality Form

Appendix C Correction/Amendment of PHI Form

Appendix D Audit Request Form

Appendix E Consent Management Form

Appendix F Annual Privacy Program Attestation

Appendix A

Plain Language Description of Health Information Network Services and Security

The following is a plain language description of the network services and security safeguards used by London Health Sciences Centre (LHSC) and St. Joseph's Health Care London (St. Joseph's) for the Supplied Services. This description provides an explanation to the health information custodians (HICs) who utilize these solutions and to the public of which health information network provider (HINP) services are being provided. It explains how security processes in place will ensure the confidentiality of the personal health information (PHI) used in the provision of such services.

Description of the Supplied Services

Cerner - The Cerner solution is suite of applications which make up the Health Information System used to electronically facilitate patient care by creating a real-time "digital chart." This chart is used by physicians, nurses and other authorized persons throughout an entire organization for all facets of patient care.

SWO DI-r - The Southwestern Ontario Diagnostic Imaging Repository (SWO DI-r), through a shared archive of imaging studies, provides a participating organization the ability to access the Diagnostic Imaging patient record using the OneView application.

PACS - Picture Archiving and Communications System (PACS) refers to a computer system that is used to capture, store, distribute and display medical images for interpretation or review. Electronic images and reports are transmitted digitally via PACS. A PACS consists of four major components: the imaging modalities such as CT and MRI, a secure network to transmit patient information, work stations for interpreting and reviewing images, and long- and short-term archives to store and retrieve images and reports.

ENITS - The ENITS solution was created to support remote access to emergent/urgent diagnostic imaging exams and to facilitate service by a specialist at one of Ontario's tertiary care centers to regional sites requesting a consultation. The consulting process is aided by CritiCall Ontario, which facilitates emergency telephone consultations between referring physicians and consulting physicians. They also notify a consulting physician when a diagnostic image has been uploaded to ENITS by a Client and document the results of the consult in accordance with their normal practices and procedures.

HINP Services

In providing services as HINP, LHSC/St. Joseph's shall provide the following information systems, information management and information technology services to enable the HICs to disclose PHI to one another:

Administrative

- Appoint Chief Privacy Officers who are the executive point of accountability (LHSC/St. Joseph's)
- Provide incident and breach management support
- Ensure all Parties comply with the terms of the Data Sharing Agreement
- Conduct privacy and security risk assessments for both product/service development and client deployments and provides a summary of the results of such assessments
- Conduct audits on behalf of the HICs to comply with legislative requirements

Technological

- Implement authorization and authentication controls to limit access to only those individuals who require it to perform their job function
- Keep electronic records to track all user accesses to PHI
- Ensure the application is encrypted and all networks are protected by devices (firewalls and routers) which limit access to and from systems

Physical

- Ensure facilities are physically secured against unauthorized access and are staffed and monitored continuously by security staff and affiliates.
- Have backup systems in place to protect against environmental issues such as power outages or hardware failures.

<ORGANIZATION LOGO>

SAMPLE PRIVACY AND CONFIDENTIALITY AGREEMENT

All residents/patients/clients under the care of <*insert organization name*> and all staff and affiliates have a right, under law, to have their health/medical/personal information treated in confidence.

This statement confirms that:

1. I have read and understand both the <*insert organization name*> corporate Privacy and Confidentiality policies.
2. I will only collect, use and disclose person health information, personal information and confidential business information required for the performance of my role.
3. I will not collect, use or disclose person health information, personal information and confidential business information if I do not need it to provide care.
4. I am aware the hospital conducts random audits on electronic systems.
5. I will ensure that I comply with the Acceptable Use of Information Technology Resources Policy by ensuring that the devices I use have administrative, technical and physician safeguards in place.
6. I will comply with the privacy legislation and regulations of Ontario.
7. I will report any privacy breaches to the Privacy Office as per the corporate Privacy Policy.
8. I understand that I must maintain all professional obligations, including adherence to the standards of practice, where there are any affiliations with regulatory colleges.
9. I understand that misuse, failure to safeguard, or the disclosure of confidential information without appropriate approvals including failure to adhere to the standards of practice where there are any professional obligations under regulatory colleges, may be cause for disciplinary action up to and including termination of employment/contract or loss of appointment or affiliation with <insert organization name>.
10. I will return corporate business information, corporate and/or personal health information at the end of my employment relationship with <*insert organization name*>.

I have completed the following Module of the Privacy and Confidentiality education program (check one):

- ☐ Professional
- ☐ Regulated Health Professional
- ☐ Clinical Support
- ☐ Non-Clinical Support

Printed Full Name: _____

Signature: _____ **Date:** _____
(YYYY/MM/DD)

Please forward your signed agreement to the Privacy Office at < *insert organization name*>.

Appendix C

CORRECTION/AMENDMENT OF PHI FORM

This form is to be used only when information requires correcting/amending at the HINP level and cannot be completed at the originating HIC(s). Please ensure all internal policies and procedures related to Corrections/Amendments are followed and the required documentation has been obtained.

PATIENT INFORMATION	
Last Name:	First Name:
Address:	Phone Number:
City, Postal Code:	Date of Birth (YYYY/MM/DD):
Hospital ID Number (if known):	Hospital and Site where PHI is located:

REQUESTING HIC CONTACT INFORMATION	
Last Name:	First Name:
Phone Number:	*Email:
Title:	Organization:

CORRECTIONS/AMENDMENTS TO BE MADE
Provide a description of PHI to be corrected/amended including all applicable details to ensure accuracy of the correction (Accession Numbers, Exam Descriptions and Dates, etc.).

☐ Proof of patient identity or legal representative has been verified.

☐ Accuracy of the request has been verified.

Please note that Ontario law does not permit hospitals to delete information from a patient's health record, even if that information is determined to be incorrect or incomplete. Instead, incorrect information is labeled as such within a patient's health record and in keeping with Ontario law it continues to remain accessible within that record.

SIGNATURE	
Signature:	Date (YYYY/MM/DD):

Please forward this document to the Regional Privacy Consultant by fax to 519-667-6706 or via secure file transfer to regionalprivacy@lhsc.on.ca to ensure confidentiality.

SUPPLIED SERVICES PRIVACY AUDIT REQUEST FORM

Please fax completed form to 519-667-6706 or via secure file transfer to regionalprivacy@lhsc.on.ca.

ORGANIZATION DETAILS

Requesting Organization: _____

Audit Requested by: _____ Date Requested: _____

SYSTEM TO BE AUDITED

☐ Cerner/OLIS ☐ OneView ☐ PACS ☐ SWODIN repository*

Date Range for Audit: _____

User: _____ Username: _____
(Last, First, Middle)

Patient: _____ MRN:_____ DOB: _____
(Last, First, Middle) (YYYY/MM/DD)

TYPE OF AUDIT (Cerner only)

Please check box next to audit being requested:

☐ **Number of Chart Opens by Patient** – provides a list of users who have viewed a specific patient's *chart* (valuable if there is a VIP, news story, etc. or if a patient wants to know who accessed their *chart*)

☐ **Number of Chart Opens by User** – provides a list of patients whose *charts* were opened by a particular user

☐ **Access by Patient and Staff and affiliates** – used to determine if a *specific user* accessed a *specific patient's* chart

☐ **Same Last Name** – used to determine whether user was accessing their own or a family member's chart

☐ **Access by Username** – allows you to view *all accesses* for a specific user

☐ **Access by Patient** – allows you to view *all accesses* for a specific patient

* SWODIN REPOSITORY

Request only when suspect access is detected in ClinicalConnect for the SWODIN viewer. Audit results can only confirm the accessions that user pulled for viewing.

Date of Access: _____ MRN: _____ Patient: _____
(Last, First, Middle)

FOR INFORMATION TECHNOLOGY SERVICES PRIVACY OFFICE USE ONLY

Received by: _____ **Date :** _____

Note: This form is not intended to be used in lieu of your corporate audit request form to document consent from patient/SDM or leadership

Appendix E

CONSENT MANAGEMENT FORM – "Lockbox"

Sites are required to follow their own internal policies when documenting patient consent using their corporate consent form and corporate processes. This form is applicable for electronic records only in HINP control.

REQUESTING ORGANIZATION INFORMATION	
Name:	Title:
Phone:	Email:
Facility:	Site:
PATIENT INFORMATION	
Last Name:	First Name:
Date of Birth (YYYY/MM/DD):	Gender:
Health Card Number:	Local PIN/MRN:

LOCKBOX DETAILS – ELECTRONIC HEALTH RECORD* (EHR)

To be used only when the site is unable to apply the Lockbox locally.

☐ Specific visit(s) _____ (YYYY/MM/DD)

☐ Range of visits _____ (YYYY/MM/DD) to _____ (YYYY/MM/DD)

☐ Lock all visits prior to this date: _____ (YYYY/MM/DD) (Future visits require a new request).

LOCKBOX DETAILS – SWODIN/OneView

Images, Reports, Exams to be locked:

Exam Date (YYYY/MM/DD)	OneView Exam Description	Accession Number	Option A	Option B	Option C
			Check the option requested		

** For a description of **Options A-C**, see Other Information section.
*** For PACS Lockbox requests, see Other Information section.

Please forward this document to the Regional Privacy Consultant by fax to 519-667-6706 or to regionalprivacy@lhsc.on.ca via secure file transfer.

OTHER INFORMATION:

* Electronic Health Record

Please note that we are only able to apply consent directives to applications for whom we are the Health Information Network Provider: EHR, SWODIN, PACS. The ENITS solution does not support consent management options as images are transitory and only stored for seven days. For all other electronic health records, please refer to the appropriate Health Information Network Provider supplying the service.

** SWODIN/OneView

Option A - Removing Image(s) Only
Capability: Viewing Clinician can view the orders and reports associated to the patient
Limitations: NONE– Procedure is reversible, this activity can be performed by local site.

Option B - Remove Reports and Image(s)
Capability: Viewing Clinician will only be able to view the orders associated to the patient (no reports or images)
Limitations: Procedure is *reversible only for participating sites that have the ability to retrigger the ORU HL7* message for that procedure.

Option C - Remove Exam/Reports and Image(s)
Capability: Viewing Clinician will be able to search and find patient and be aware that imaging has been performed but the description is replaced with "Patient Requests Lockbox-Consent Directive". Report and Images will be removed.
Limitations: Procedure is *reversible only for participating sites that have the ability to retrigger the ORU HL7* message for that procedure.

*** PACS

The technical ability to apply a Lockbox in PACS is available to local PACS Administrators only. If you are unable to reach a PACS Administrator at your site, the LHSC/SJHC PACS Administrators can be contacted for assistance by contacting the LHSC Help Desk at 519-685-8500 x44357.

LOCAL PRIVACY OFFICER OR AGENT SIGNATURE	
Signature _____	Date _____
VERIFICATION OF PATIENT/SDM'S IDENTITY:	
Form of identification:	
☐ Driver's License ☐ Passport	☐ Notarized letter/Lawyer's letter ☐ Health Card or Other _____
ID verified by: _____ (NAME)	_____ (DATE)

FOR INFORMATION TECHNOLOGY SERVICES PRIVACY OFFICE USE ONLY

Received by: _____ **Date :** _____

Please forward this document to the Regional Privacy Consultant by fax to 519-667-6706 or to regionalprivacy@lhsc.on.ca via secure file transfer.

Appendix F

ANNUAL PRIVACY PROGRAM ATTESTATION

As a participant in a shared system, the accountability for personal health information is also shared. PHIPA section 12(1) describes our duty to protect PHI, and as an administrative safeguard, all participants are asked to attest that they are in compliance with all legislative and regulatory requirements as applicable to our individual information practices.

Attestation Questions	Reference (PHIPA, Regulations, Orders)	Status	
		Yes	No
Designated Privacy Officer	PHIPA Section 15(2), (3)		
Written Public Statement that is available to the public as well as education material (brochures, posters, website, etc.)	PHIPA Section 16(1), 18(6)		
Annual privacy education and training of staff, physicians, students, volunteers and contracted staff.	PHIPA Section 15(3)(b) Principle 1: Accountability		
Process for tracking completion of education and Confidentiality Agreements.	Decision 102 Principle 1: Accountability		
Auditing (including process to audit individuals with high risk of breach, e.g. "VIPs")	PHIPA Section 12(1)		
Privacy policy	Sec. 10		
Confidentiality policy	Sec. 10		
Identity and Access Control policy	Sec. 11.1, 17(1)(b)		
Security of Confidential Information & Information Technology Systems policy	Sec. 12(1)		
Remote Access policy	Sec. 12(1)		
Observer/Vendor Representative policy	Sec. 12(1)		
Breach of Privacy policy	Sec. 12(2), 16(2)		
Breach Management process	O. Reg. 329/04, s.6.3 (1) (2)		
Process for notifying a professional college in the event of a confirmed privacy breach.	Sec. 17.1 (2-5)		
Records Retention and Disposal policy	Sec. 13(1)		
Retention Schedule	Sec. 13(2)		
Access to PHI policy	Sec. 52(1)		
Disclosure of PHI policy	Sec. 38-50		
Correction of PHI policy	Sec. 55(1-13)		
Consent Directives policy and process	Sec. 19(1)(2), 38(1)(3)		
Document/brochure that explains the consent directives process including instructions for applying these restrictions in other external systems (eHealth applications, eCHN, etc.).	Sec. 18 (6), 21 (1)(b) Decision 102		
Process to document when an override of a consent directive has occurred to eliminate or reduce a significant risk of serious bodily harm	Sec. 40(2)		
Policy or procedure to allow patients to restrict collection, use, or disclosure of their PHI for fundraising purposes.	Sec. 32(1)		

Please complete this form and return to the Regional Privacy Consultant by March 31st.

Attestation Questions	Reference (PHIPA, Regulations, Orders)	Status Yes	Status No
Process for managing consent when an individual requests to withhold/withdraw religious affiliation information.	Sec. 20(4)		
Use of PHI for Research, Education, Quality Assurance and Risk Management policy	Sec. 44(1-6), 37(1)(c-j), 37(3)		
Access Request Process (Release of Information), including a process for verifying an individual's identity for access/disclosure requests.	Sec. 11(2) Sec. 54(9)		
Breach Management process	Sec. 12(2), 16(2)		
Designated person and process for managing privacy audits provided by the HINP.	Sec. 12(1)		
Requirement that all portable devices that may contain PHI/CI be encrypted.	Sec. 12(1)		
Method of transferring PHI/CI securely to 3rd parties such as secure file transfer or FTP.	Sec. 10(1), 12(1)		
Agreements with any 3rd party document destruction companies that outline the safeguards in place to protect PHI.	Sec. 13(1)		
Substitute Decision Maker (SDM) identification process in cases where the individual is deemed incapable.	Sec. 22(3)		
Guidelines about what types of information can be disclosed about an individual to another individual whether in-person or via telephone (i.e. family or friends).	Sec. 38(3)		
Process for handling complaints which includes a direction to contact the IPC if the individual choses to do so.	Sec. 54(8)		
Process in place to log all inappropriate collections, uses, disclosures so they can be reported to the IPC on or before the March deadline each year.	O. Reg. 329/04, s. 6.4 (1)(2)		

Comments:
Include any additional information that may be required to explain your answers.