Applies to: All Hamilton Health Sciences (HHS) staff including members of the medical, dental and midwifery staff, affiliates, contractors, researchers, volunteers, hospital affiliates and learners.

1.0 Purpose
1.1 Hamilton Health Sciences (HHS) complies with the Personal Health Information Protection Act, 2004 (PHIPA) and the obligations that apply to Health Information Custodians (HIC), as defined under PHIPA.
1.2 PHIPA is Ontario’s health-specific privacy law, which sets out the rules for the collection, use and disclosure of Personal Health Information (PHI) about individuals. Such rules are designed to protect the confidentiality of PHI and the privacy of individuals, while facilitating the effective provision of health care. PHIPA grants certain rights to individuals in respect of their PHI and places certain obligations on HHS to enable its patients to exercise their rights and resolve any complaints in respect of its privacy practices.
1.3 This Policy sets out the applicable rights and obligations under PHIPA that HHS Staff must be aware of and identifies the additional privacy policies and standards that HHS has established to respect patient rights and discharge its obligations under PHIPA.
1.4 HHS Staff must comply with all HHS Privacy policies and procedures. Instances of non-compliance will be reviewed by the HHS Privacy Office. Such violations will be subject to disciplinary actions, up to and including termination of employment and may also be subject to temporary or permanent loss of access privileges.

1.2 Policy Scope
1.2.1 This Policy outlines HHS’ key privacy-related rules and in particular those concerning:
   - Collecting, using and disclosing PHI;
   - Patient rights with respect to their PHI;
   - Safeguarding PHI and managing suspected or actual privacy incidents;
   - Reviewing and resolving complaints by patients in respect of HHS’ privacy practices; and
   - Training and awareness in respect of HHS’ privacy practices.

See Appendix - Glossary for the defined terms used in this Policy.

2.0 Policy
2.1 The Collection, Use and Disclosure of Personal Health Information

2.1.1 Accountability
Accountability for HHS compliance with privacy principles rests with the Board and/or CEO, having overall accountability, although other individuals within HHS are responsible for the day-to-day collection and processing of personal health information.

2.1.2 The Chief Privacy Officer is delegated to act on behalf of the CEO with respect to the oversight and compliance of privacy at HHS.

2.1.3 HHS is responsible to protect the privacy of PHI in its custody or control. PHI that has been transferred to an agent of HHS will be protected through the use of contractual or other means.

2.1.4 HHS implements policies and guidelines to give effect to this policy and the principle of accountability.
2.2 Consent
2.2.1 HHS will not collect, use or disclose a patient’s PHI without their consent unless otherwise permitted or required by law.
2.2.3 In most cases, PHI will be collected, used or disclosed by HHS Staff for the purpose of providing or assisting in the provision of health care. In such cases, HHS Staff may rely on the implied consent of the patient to collect, use and disclose PHI. Implied consent may not be relied on when disclosing PHI:
- To a person or entity that is not a Health Information Custodian (HIC)
- For a purpose other than providing or assisting in providing health care, or
- Where a patient has expressly limited their consent
2.2.4 When treating children and adults who cannot understand what it means to give or withhold consent, HHS Staff will obtain consent from a substitute decision-maker (Substitute Decision-Maker or SDM).
2.2.5 When consent is required for the collection, use or disclosure of information about a child under 12, HHS will obtain consent from that child, if the child is capable of making their own health care decisions in accordance with applicable law, or from their parent or other lawful guardian as required.
2.2.6 In accordance with section 33 of PHIPA, HHS will only collect, use or disclose PHI for the purpose of marketing or for market research with express consent. Collection, use or disclosure of PHI for fundraising purposes will only be done in accordance with section 32 of PHIPA and applicable regulations.
2.2.7 Patients are entitled to withdraw consent to the use and disclosure of their PHI by placing a lock-box on their personal health record. Lock-boxes may only be overridden for purposes authorized by law. All cases involving an override of a lock-box will be reviewed by the HHS Privacy Office.

2.3 Exceptions to the General Requirement for Consent
2.3.1 The general requirement to obtain consent from a patient is subject to limited exceptions. There may be certain instances, such as legal, medical, or security reasons, where HHS and HHS Staff may collect, use and/or disclose PHI without consent.
2.3.2 There are certain circumstances where consent is not required for use and disclosure of PHI (e.g. for certain research purposes including those referred to in section 44(3)(d) of PHIPA, or to determine patient eligibility).

2.4 Limiting the Collection, Use and Disclosure of Personal Health Information
2.4.1 HHS and HHS Staff shall respect the principle of data minimization and shall only collect, use and disclose the amount of PHI that is reasonably necessary to meet the purpose of the collection, use or disclosure.

2.5 Disclosure of Personal Health Information
2.5.1 HHS may disclose PHI with the implied consent of an individual to other HICs within the patient’s Circle of Care for the provision of health care for such individual.
2.5.2 HHS may also disclose PHI in other limited circumstances, such as when:
- The recipient has obtained consent in accordance with PHIPA;
- The recipient is using PHI for HHS approved health care and health systems analytics;
- The disclosure is otherwise authorized by law (e.g. the recipient is a researcher who satisfies the requirements under section 44 of PHIPA (see section 3.1.3 above) or disclosures to Prescribed Entities in accordance with section 45 of PHIPA); or
2.5.3 HHS may disclose PHI to a person outside of Ontario in accordance with PHIPA.

2.6 Ensuring Accuracy of Personal Health Information
2.6.1 HHS is required by law to take reasonable steps to ensure that those who access patient PHI through HHS systems use information that is accurate, complete and up-to-date. HHS Staff must take reasonable steps to ensure that the PHI of patients remains accurate, complete and up-to-date. HHS and HHS Staff must take reasonable steps to ensure that any PHI disclosed to another person or entity is as accurate, complete and up-to-date as is necessary for the purposes of the disclosure or must clearly set out the limitations on the accuracy

2.7 Responding to Patients’ Requests
2.7.1 Subject to limited exceptions, patients are entitled to access and correct their health record and PHI. HHS must respond to any such requests without undue delay. HHS Staff must facilitate such requests in accordance with the PRI - Policy for Responding to Requests for Access, Correction and/or Disclosure of Personal Health Information.

2.8 Safeguarding Personal Health Information
2.8.1 HHS must take reasonable steps to ensure that PHI is protected against theft, loss and unauthorized access, use or disclosure, and that records containing PHI are protected against unauthorized copying, modification or disposal.
2.8.2 HHS only permits authorized staff and, in some circumstances, external consultants or other authorized service providers, to access and use PHI on a strict “need-to-know” basis, that is, when and to the extent required to perform their duties and/or services, and only after they have entered into a contractual arrangement with HHS and completed the mandatory training requirements in the areas of privacy and security.
2.8.3 HHS provides training to ensure that all HHS Staff understand the rules relating to use of HHS’ health information system, including but not limited to EPIC. In particular, HHS Staff must ensure that they understand how to apply the ‘Circle of Care’ concept. Furthermore, HHS’ health information system is not to be used by HHS Staff to look up their own health information or that of their family and friends. MyChart and other web-based portals are available for such look-ups. Intentional use of HHS’ health information systems EPIC and Clinical Connect) in this manner is a breach of PHIPA, this Policy, and in some instances a violation of professional codes of conduct, and will result in disciplinary action.
2.8.4 HHS remains accountable for PHI that is provided to service providers.
2.8.5 All HHS Staff must comply with all applicable laws and regulations, and with HHS requirements that relate to the handling and safeguarding of PHI including requirements reflected in the PRI - Use of Mobile Devices for the Collection, Use, and Disclosure of Personal Health Information Policy.
2.8.6 HHS conducts regular auditing and monitoring activities to detect any inappropriate or unauthorized access to PHI. Auditing and monitoring activities are conducted in accordance with the PRI - Auditing and Monitoring of Personal Health Information Protocol.
2.8.7 If unauthorized access is suspected or confirmed, the Privacy Office will initiate the PRI - Privacy Incident Readiness and Response Policy and the PRI - Privacy Breach Investigation Protocol.

***These documents are for internal use only at Hamilton Health Sciences (HHS) and are CONTROLLED documents. As such, any documents appearing in any format (paper or electronic) found outside of the HHS Policy and Document Library, are not controlled and should ALWAYS be checked against the version on the Policy and Document Library intranet prior to use to ensure this document is current. Only the documents contained on the Policy and Document Library site are official HHS approved versions. No modifications to these documents (including conversion of forms to fillable format) are permitted. ***
Managing and Responding to Privacy Incidents

2.9.1 HHS must notify HHS patients upon the theft, loss, unauthorized access, use or disclosure of PHI (a "Privacy Breach"). In certain circumstances, HHS may also be required to notify the Information and Privacy Commissioner of Ontario (IPC) about a Privacy Breach.

2.9.2 HHS Staff must immediately report all suspected or confirmed Privacy Incidents to the HHS Privacy Office. Privacy Incidents will be dealt with in accordance with the PRI - Privacy Incident Readiness and Response Policy.

Retention, Archiving and Destruction of Personal Health Information

2.10.1 HHS must retain, archive and destroy PHI in accordance with PHIPA.

2.10.2 HHS must ensure that PHI that is the subject of a request for access or correction is retained for as long as necessary to allow the individual to exhaust any recourse they may have under PHIPA.

2.10.3 Individuals responsible for the archiving or secure destruction of PHI must be properly trained in methods that correspond to the format, media or device, in accordance with legal requirements, industry best practices, and HHS standards.

Privacy Impact Assessments

2.11.1 Privacy impact assessments (PIAs) will be undertaken by HHS in respect of new or existing programs or systems’ collection, use and disclosure of PHIPA in order to provide a framework to ensure that privacy is considered throughout their design. PIAs also assess the program or system’s compliance with PHIPA, FIPPA, other applicable laws, HHS policies, contractual obligations and industry best practices.

2.11.2 HHS Staff involved in new initiatives and research projects in which PHI is collected, used, disclosed, retained, stored or transferred through the use of digital technology, including but not limited to applications, software, cloud or web-based platforms, are responsible for ensuring that a PIA is conducted when required and must review the PRI - Privacy Impact Assessments Policy.

Responding to Patient Inquiries and Complaints

2.12.1 Patients have the right to make inquiries and/or complaints in relation to HHS’ privacy policies, procedures and practices and compliance with PHIPA and its regulations. HHS Staff who receive such privacy inquiries or complaints are responsible for directing patients to the HHS Privacy Office as soon as practicable.

2.12.2 The HHS Privacy Office must respond to all privacy inquiries and complaints as soon as practicably possible, and no later than within 30 calendar days. In limited circumstances, the HHS Privacy Office can notify the patient that it requires an additional time to respond to an inquiry or complaint. For more information, see the PRI - Privacy Inquiries or Complaints Protocol.

Openness and Transparency

2.13.1 HHS is committed to being open and transparent about its PHI practices. Accordingly, the HHS Privacy Office will ensure that appropriate information is made available to the public in a clear and accessible manner, including the following information that is made accessible through the HHS website:

- HHS’ Patient Privacy Statement; and
- Information about how a patient may access their PHI records, correct inaccuracies in their patient records and otherwise make inquiries and/or complaints to HHS or the Information and Privacy Commissioner of Ontario (IPC) about HHS’ PHI practices.

***These documents are for internal use only at Hamilton Health Sciences (HHS) and are CONTROLLED documents. As such, any documents appearing in any format (paper or electronic) found outside of the HHS Policy and Document Library, are not controlled and should ALWAYS be checked against the version on the Policy and Document Library intranet prior to use to ensure this document is current. Only the documents contained on the Policy and Document Library site are official HHS approved versions. No modifications to these documents (including conversion of forms to fillable format) are permitted.***
2.14 HHS Staff Training and Awareness
2.14.1 HHS will make available privacy and security training to inform all HHS Staff of their obligations under PHIPA and the HHS Privacy policies and procedures. Such training must be completed by each individual HHS staff member initially upon being hired or engaged and, at minimum, annually thereafter (if applicable). HHS Staff are also required to sign a Confidentiality Pledge upon being hired or otherwise engaged by HHS and annually thereafter.

2.15 Enforcement
2.15.1 HHS Staff must comply with all HHS Privacy policies and procedures. Instances of non-compliance with this Policy (as well as associated policies referred to above) will be reviewed by the HHS Privacy Office in consultation with Human Resources. Such violations will be subject to disciplinary action, up to and including termination of employment and may also be subject to temporary or permanent loss of access privileges and/or legal sanctions.
2.15.2 HHS Staff must notify the HHS Privacy Office at the first reasonable opportunity of any known or suspected breach of this Policy.
2.15.3 Failure to comply with this Policy (as well as associated policies referred to above) may result in, but is not limited to:

- Denial of access to HHS’ information systems;
- Contractual remedies, as may be appropriate for third party suppliers, consultants and/or contractors, such as termination of contract; and/or
- Disciplinary action for staff, up to and including termination of employment and/or suspension or revocation of hospital privileges with HHS

3.0 Procedure
3.1 The HHS Privacy Office is responsible for implementing procedures in support of this policy.

4.0 Definitions
See Appendix - Glossary

5.0 Cross References
PRI - Policy for Responding to Requests for Access, Correction and/or Disclosure of Personal Health Information
PRI - Use of Mobile Devices for the Collection, Use, and Disclosure of Personal Health Information Policy
PRI - Auditing and Monitoring of Personal Health Information Protocol
PRI - Privacy Incident Readiness and Response Policy
PRI - Privacy Impact Assessments Policy
PRI - Patient Privacy Inquiries or Complaints Policy

6.0 Other HHS References
N/A

7.0 External References
Personal Health Information Protection Act, 2004 (PHIPA)
8.0 Developed By
HHS Privacy Office

9.0 In Consultation With
HHS Patient Experience
HHS Human Resources
HHS Labour Relations

10.0 Approved By
Chief Privacy Officer

11.0 Appendix
See Appendix - Glossary
Appendix - Glossary

Agent – in relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent’s own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the agent is being remunerated.

Break The Glass (BTG) – is an Epic security feature that allows HHS to restrict user access to certain patient records, either at the encounter level or at the patient level. The BTG box will appear when a patient has requested a Consent Directive, or "Lockbox", to restrict access to information within their records from HHS.

Bump The Glass – Attempted access is known as "bumping the glass" to patient records. Bumping the glass occurs when a user attempts to access the patient record, is prompted to break the glass, and then cancels the access attempt.

Circle of Care – A group that includes any person who is involved in the care or treatment of a given patient and who may rely on implied consent for the collection, use, and disclosure of information for the purposes of providing that patient with care

Confidentiality Pledge – means the attestation HHS Staff must sign after successfully completing their initial and annual privacy trainings.

Health Information Custodian (HIC) – means a person or organization (as listed in PHIPA) that has custody, or control of PHI as a result of or in connection with performing the person’s or organization’s powers or duties or work. The term is fully defined in section 2 of PHIPA and it includes:

- A health care practitioner or a person who operates a group practice of health care practitioners.
- A service provider within the meaning of the Home Care and Community Services Act, 1994 who provides a community service within the meaning of that Act.
- A person who operates one of the following facilities, programs or services:
  - A hospital, a psychiatric facility or an independent health facility
  - A long-term care home
  - A retirement home
  - A pharmacy
  - A laboratory or a specimen collection centre
  - An ambulance service
  - A home for special care
  - A centre, program or service for community health or mental health whose primary purpose is the provision of health care
- A medical officer of health of a board of health
- The Minister, together with the Ministry of the Minister, if the context so requires

HHS Staff – refers to all individuals or groups who provide services to Hamilton Health Sciences unless otherwise specified, including full-time, part-time and temporary employees of HHS, including members of the medical, dental and midwifery staff, individuals working at HHS on secondment, volunteers, students, contractors, researchers, hospital affiliates and certain external professional services consultants or providers.
**Information and Privacy Commissioner (IPC)** – means the Information and Privacy Commissioner of Ontario appointed under the *Freedom of Information and Protection of Privacy Act* (as defined in [PHIPA](#)).

**Personal Health Information (PHI)** – means any identifying information, in the custody or under the control of HHS, about an individual in either oral or recorded form that relates to the physical or mental health of an individual; or relates to the provision of health care to the individual, including the identification of a person as a provider of health care to the individual (as defined in section 2 of [PHIPA](#)).

**Personal Information (PI)** – means any information about an identifiable individual such as personal health information, health workforce personal information and employee personal information (as defined in section 2 of [PHIPA](#)).

**Personal Health Information Protection Act, 2004 (PHIPA)** – means the Ontario *Personal Health Information Protection Act, 2004* and associated regulations.

**Privacy Impact Assessment** – a “self-assessment” tool that provides an evaluation of a program, initiative, process, system or other technology implementation and is intended to identify and mitigate privacy risks.

**Privacy Breach** – A privacy breach is any collection, use or disclosure of PHI that is not in compliance with PHIPA and its regulation, including:

- The collection, use and disclosure of PHI that is not in compliance with PHIPA or its regulations;
- Circumstances where PHI is stolen, lost or subject to unauthorized use or disclosure or where records of PHI are subject to unauthorized copying, modification or disposal;
- A contravention of one or more of HHS’s privacy policies, procedures or practices of HHS involving the collection, use or disclosure of PHI; and
- A contravention of privacy provisions of agreements entered into by HHS, including research agreements, confidentiality agreements and agreements with third party service providers, and data sharing agreements retained by the HHS.

**Privacy Incident** – means any actual or suspected collection, use, storage or disclosure of PHI that is not in compliance with PHIPA, including the loss, theft or unauthorized copying, access, use, disclosure, modification, or disposal of any PHI.

**Substitute Decision-Maker (SDM)** – in relation to an individual, means, unless the context requires otherwise, a person who is authorized under PHIPA to consent on behalf of the individual to the collection, use or disclosure of PHI about the individual (as defined in section 2 of [PHIPA](#)).

**Keyword Assignment**

| Keyword Assignment | PHIPA, PHI, circle of care, breach, incident, privacy, |