St. Joseph's Healthcare Hamilton	Manual Corporate	Section ADMIN	Type Policy & Procedure	Pages 1-13	Number 178-ADM
Subject: Privacy Policy				Date: 23/02/2022	
Supersedes: NEW *Replaces 090-ADM & 092 ADM*	Cross Reference: 167-ADM, 169-ADM, 012-HIM, 149-ADM			Issuing Authority: Department of Risk, Legal & Privacy	
☒ Charlton Campus ☒ King Campus		☒ West 5th Campus ☒ All Sites of Program			

This policy applies to all employees, members of the professional staff, volunteers, learners, contractors and all persons who have a relationship with SJHH

Table of Contents

1.0 Purpose and Goals

St. Joseph's Healthcare Hamilton (SJHH or the hospital) is committed to protecting the privacy of our patients and safeguarding the personal health information (PHI) and personal information (PI) with which we are entrusted. SJHH's obligations in regards to personal health information are outlined in the *Personal Health Information Protection Act, 2004* (PHIPA), and obligations in

regards to personal information are prescribed by the *Freedom of Information and Protection of Privacy Act* (FIPPA).

In the course of carrying out its patient care, research, teaching and administrative functions SJHH collects, retains, uses, discloses, and ultimately disposes of PI and PHI relating to its patients and staff, within its custody and control.

Our privacy standards are based on legal and regulatory requirements and the Canadian Standards Association Model Code for privacy which outlines ten specific principles for protecting privacy.

2.0 Definitions

Agent: any person authorized by SJHH to act on its behalf in respect of PHI, PI or confidential information for SJHH's purposes, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, is employed by the custodian, or is being remunerated.

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.

Collection: The process of gathering, acquiring, receiving or obtaining personal information, personal health information or private and confidential information, whether directly from the person or patient, or from any other source such as tests, images, samples, specimens or other care providers. Generally, information is considered to be collected the first-time information is gathered, acquired, received or obtained. Any viewing, handling or otherwise dealing with the information after the initial collection is generally considered to be a use.

Consent: A patient or substitute decision maker's (SDM) agreement, whether express (explicit statement from the patient or SDM) or implied (concluded from the surrounding circumstances), written or oral, to the collection, use, or disclosure of their PHI or PI.

Disclosure: To make information available or to release it to any other person.

Health Information Custodian: A person or organization described in section 3 of the *Personal Health Information Protection Act* (PHIPA) and who has custody or control of PHI. For the purposes of this policy, this includes SJHH.

Personal Health Information (PHI): information about an individual, whether in oral or recorded form, that identifies the individual or could enable such identification and that relates to: the person's physical or mental health, medical history or past or future medical treatment, including the identity of a patient's healthcare provider or a patient's health number. For the purpose of this policy, PHI has the same meaning as defined in Section 4 of PHIPA.

Personal Information (PI): Recorded information about an identifiable individual. For the purpose of this policy, personal information (PI) has the same meaning as defined in Section 2 of FIPPA.

Privacy Breach: any intentional or unintentional unauthorized collection, use, or disclosure of PHI or PI, including the loss of or failure to protect such information.

Secondary Use: Any use of information beyond that for which the information was collected.

Staff: Includes all permanent or temporary, casual or contract, employees, trainees and volunteers, including but not limited to physicians, residents, interns, researchers and students.

Substitute Decision-Maker (SDM): a person who is authorized under PHIPA to consent on behalf of a patient to the collection, use, or disclosure of that patient's PHI.

Use: To view, handle or otherwise deal with information.

3.0 Equipment/Supplies

None.

4.0 Policy

4.1 Principle 1 – Accountability for Personal Information (PI) and Personal Health Information (PHI)

SJHH is responsible for PI/PHI under its custody or control and has designated a Chief and the Department of Risk, Legal & Privacy as responsible for privacy (Privacy Contact). The Privacy Contact is accountable for the hospital's overall compliance with privacy legislation, and the Privacy Contact's duties may include:

- periodic assessments of information collection, use and disclosure practices;
- developing policies, procedures and tools to carry out a hospital wide Privacy Compliance Program;
- overseeing, conducting and setting out requirements for ongoing staff privacy training;
- directing the notification of patients or their SDMs of any loss theft, or unauthorized access, use or disclosure of PHI as required by PHIPA.

SJHH will have in place and maintain policies, procedures and practices in respect of privacy that are necessary to enable it to comply with their obligations under PHIPA, FIPPA and other privacy legislation where applicable.

SJHH will use contractual or other means to provide a comparable level of protection for information that has been transferred to a third-party for processing.

Audits will be conducted periodically on records of a confidential nature to evaluate the appropriateness of the collection, use and disclosure of PHI / PI by staff and agents and to monitor compliance with this policy.

4.2 Principle 2- Identifying Purposes for the Collection for Personal Information or Personal Health Information

SJHH, at or before the time PI/PHI is collected, will identify the purposes for which this information is collected, used, disclosed, and retained. The main purposes are:

- delivery of patient care;
- administration and management of the hospital, including the hiring and credentialing of staff;
- education of SJHH staff and trainees;
- HIREB approved research;
- statistics and quality improvement;
- compliance with legal and regulatory requirements.

Contact information (e.g. names and addresses) may also be used for other purposes such as:

- fund-raising to support priorities of the hospital; and
- patient satisfaction surveys to evaluate and improve the quality of care.

4.3 Principle 3 – Consent for the Collection, Use and Disclosure of Personal Information or Personal Health Information

PHIPA permits SJHH to rely on a patient's or SDM's implied consent for the collection, use, and disclosure of PHI if the information is required for the purposes of providing healthcare to the patient.

Before using PHI for any secondary purpose, the express consent of the patient or their SDM is to be obtained except where the information:

(i) Is needed to prevent serious bodily harm or reduce a significant risk of harm to any person;
(ii) Is being collected for the purpose of educating SJHH staff or agents on the provision of healthcare;
(iii) Is being used to manage risks and errors or to improve the quality of healthcare services;
(iv) Is being used and disclosed as part of a research study that has been approved by the Hamilton Integrated Research Ethics Board (HIREB) or other contractually assigned Board of record as approved by SJHH; or
(v) is required or permitted to be disclosed by law.

When obtaining consent from patients or SDMs, SJHH Staff and Agents must make reasonable efforts to ensure that patients or their SDMs are advised of the purpose for which their information is being collected.

Patients or their SDMs are entitled to withdraw consent to the use and disclosure of their PHI stored in SJHH's electronic health record (Dovetale) system by applying a consent directive (lockbox). We may only override a consent directive with patient consent or for authorized purposes.

4.4 Principle 4 – Limiting Collection of Personal Information or Personal Health Information

The amount and type of PI/ PHI collected shall will be limited to that which is necessary for the purposes identified by SJHH. Information will be collected by fair and lawful means.

4.5 Principle 5 – Limiting Use, Disclosure, and Retention of Personal Information or Personal Health Information

PI/PHI will not be used or disclosed for purposes other than those for which it was collected, except with the express consent of the individual,

for a Research study approved by HIREB or another approved Board of record, or as permitted or required by law. All PI / PHI shall be retained as required by law, and SJHH shall have policies / procedures in place with respect to the retention of PI / PHI. Only those individuals who need a record of PI/PHI in the performance of work duties shall access it.

4.6 Principle 6 – Accuracy of Personal Information or Personal Health Information

SJHH will take reasonable steps to ensure that information about patients is accurate, complete, and up-to-date. PHI will be recorded when it is collected or as soon as reasonably possible afterward. Whenever possible, the individual who collects the PHI should be the one recording the PHI. Professional, regulatory and industry standards will be adhered to, as applicable. When disclosing PHI for any purpose, we will set out for the recipient any known limitations on the accuracy and/or completeness of the information.

4.7 Principle 7 – Ensuring Safeguards for Personal Information or Personal Health Information

SJHH will safeguard the PHI / PHI collected, used, and disclosed in the course of authorized duties through the use of physical, administrative, technical, and electronic safeguards.

All known, suspected, or potential privacy breaches must be reported to the Privacy Office within the Department of Risk, Legal & Privacy as soon as reasonably possible. The Manager of the individual or department named will be contacted in order to help investigate and manage the breach.

Any SJHH Staff who violates this policy will be subject to disciplinary action up to and including immediate suspension or termination of employment with SJHH, or in the case of members of the medical staff, up to and including suspension or termination of hospital privileges. The existing channels for appealing such decisions apply. Under PHIPA, SJHH also has mandatory privacy breach reporting requirements to the Information & Privacy Commissioner of Ontario (IPC) as well as to relevant regulatory colleges. SJHH may exercise its discretion to terminate the placement of a student volunteer or observer upon a breach of this policy. Sanctions for Staff that violate this policy, PHIPA and/or FIPPA are set out in Appendix B – Privacy Sanction Guidelines.

4.8 Principle 8 – Openness about Personal Information or Personal Health Information Policies and Practices

SJHH will make readily available to individuals, information about its policies and practices relating to the management of PI/PHI. New SJHH Staff and any other individual doing work at SJHH will be made aware of this policy during their orientation to SJHH.

4.9 Principle 9 – Individual Access to their own Personal Information or Personal Health Information

Upon request and verification of identity, patients or their SDMs will be informed of the existence, use, and disclosure of their PHI and given access to that information within 30 days unless a specific exception applies.

Staff who have authorized access to clinical systems are prohibited from directly accessing their own PHI or PHI of any relative for whom they may have access rights. Access may only be obtained through registering for and/or obtaining proxy access to MyChart, a secure patient portal, or through Health Records Department processes.

When an individual demonstrates the inaccuracy or incompleteness of their PHI held by SJHH, steps will be taken to review and amend the information.

4.10 Principle 10 – Challenging Compliance

An individual will be able to lodge a privacy complaint regarding the above principles to the Privacy Contact, or appropriate designated individual. SJHH will investigate all complaints. If a complaint is found to be justified, SJHH will take appropriate measures. Complaints may also be lodged with the IPC.

5.0 Procedure

Procedure for privacy breach management set out in Appendix A- Privacy Breach Protocol.

6.0 Documentation

None.

7.0 References

- Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c.F.31
- Personal Health Information Protection Act, 2004, S.O. 2004, c.3 Sched. A
- Information and Privacy Commissioner of Ontario, "Detecting and Deterring Unauthorized Access to Personal Health Information" (Toronto: ON, 2015)

8.0 Author(s)

Chief Risk, Legal & Privacy Officer

9.0 Sponsor

Chief Risk, Legal & Privacy Officer

10.0 In Consultation With

- Risk Management
- Digital Solutions
- Human Resources
- Public Affairs
- Professional Advisory Committee
- Medical Advisory Committee
- Executive Leadership Team

11.0 Posting Dates

Initial Posting Date: February 25, 2022

Posting Date History:

12.0 Scheduled Review Date

February 2025