CORPORATE
GEN002

Policy:	Privacy	
Owner:	Director, Patient Relations, Security Services and Chief Privacy and Risk Officer	
Sponsor:	Vice President, Patient Care and Risk Management	
Approval by:	Senior Leadership Team	**Date:** 2022-05-25
Original Effective Date: 2004-01-22	**Reviewed Date:** 2024-08-27	**Revised Date:** 2022-05-25

This policy applies to: ☒ St. Joseph's Health Care London
or
☐ Mount Hope Centre for Long-Term Care
☐ Parkwood Institute Main Building
☐ Parkwood Institute Finch Family Mental Health Care Building
☐ St. Joseph's Hospital
☐ Southwest Centre for Forensic Mental Health Care

(If this policy applies to all sites, please check St. Joseph's Health Care London only.)

POLICY

St Joseph's Health Care London (St Joseph's) is responsible to comply with the Personal Health Information Protection Act (PHIPA), 2004 and, as such, is a Health Information Custodian responsible for personal health information (PHI) in its custody and control, i.e. all PHI collected about registered patients of the organization that is used, disclosed and retained for any purpose, including patient care, education, research and administrative purposes. St. Joseph's obligation includes information transferred to a third party.

As a Health Information Custodian St Joseph's is responsible to have a Privacy Program, a Corporate Privacy policy and make a public friendly version of the policy available to patients. The Corporate Privacy policy is the foundation for St Joseph's information practices, other policies and procedures, and sets the standard upon which the organization collects, uses, discloses and retains PHI.

St Joseph's strives to be PHIPA compliant, is committed to a high standard of privacy for its information practices and has adopted the National Standard of Canada Model Code for the Protection of Personal Information:

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure, and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Patient Access
10. Challenging Compliance

PHIPA grants privacy rights to the patient/client/resident or an incapable patient's Substitute Decision Maker (SDM) (hereafter referred to as the patient/SDM)

Principle 1 - Accountability for PHI
St Joseph's is legally accountable for PHI in its custody and control and has designated responsibility to the Director, Patient Relations, Security Services and Chief Privacy and Risk Officer to set privacy and confidentiality standards and to put measures in place to make staff and affiliates aware of their privacy and confidentiality obligations.

St Joseph's meets this requirement by implementing the following policies and processes:

- Privacy
- Confidentiality
- Breach of Patient Privacy
- Corporate Procurement of Consulting Services
- Corporate Procurement of Goods and Non-Consulting Services
- Education of staff and affiliates including St. Joseph's mandatory education programs.

Principle 2 - Identifying Purposes for the Collection of PHI
At or before the time PHI is collected, St Joseph's makes a patient/SDM aware of the purposes for which PHI is collected. The organization collects PHI for the delivery of patient care, the administration of the health care system, research, education, quality assurance, fundraising, and to meet our legal and regulatory requirements.

A patient/SDM has the right to consent, refuse or place restrictions on the collection, use and/or disclosure of PHI, unless the collection, use or disclosure is permitted or required by law.

St Joseph's meets this requirement by implementing the following policies and processes:
- Access and Disclosure of Personal Health Information
- Use of Personal Health Information for Research, Education and Quality Assurance
- Posted notices and brochures informing patients/SDMs about the purpose for the collection, use and disclosure of their health information and how to contact the St. Joseph's Patient Relations, Privacy and Risk.
- Information on the St Joseph's Privacy Internet site for patients/SDMs including a public-friendly version of the Privacy policy

Principle 3 - Consent for the Collection, Use, and Disclosure of PHI
St Joseph's obtains knowledgeable consent of the patient/SDM for the collection, use, or disclosure of PHI, except where inappropriate. The form of consent (i.e. implied or express) depends on the purpose of the collection, use and/or disclosure and the intended recipient of the information. Information is collected by fair and lawful means. PHI can be collected, used, or disclosed without the knowledge and consent of the patient/SDM only where permitted or required by law.

A patient/SDM may withdraw or restrict consent at any time, unless the collection, use or disclosure is permitted or required by law. St Joseph's informs the patient/SDM of the implications of such withdrawal.

St Joseph's meets this requirement by implementing the following policies and processes:
- Access and Disclosure of Personal Health Information
- Use of Personal Health Information for Research, Education and Quality Assurance
- Addressing Requests from Patients Who Wish to be Anonymous
- Patient Requests to Restrict the Use and Disclosure of Personal Health Information

Principles 4 and 5 - Limiting Collection, Use, Disclosure, and Retention of PHI
St Joseph's limits collection, use, disclosure and retention of PHI to only what is required to fulfill the purposes identified to the patient/SDM and for which consent was obtained, except with the consent of the patient/SDM, or as required by law.

St Joseph's meets this requirement by implementing the following policies and processes:
- Use of Personal Health Information for Research, Education and Quality Assurance
- Disclosure of Patient Information, Samples and/or Belongings to Law Enforcement Agents
- Addressing Requests from Patients Who Wish to be Anonymous
- Records Retention and Destruction
- Patient Requests to Restrict the Use and Disclosure of Personal Health Information

Principle 6 - Ensuring Accuracy of PHI
St Joseph's is responsible to ensure that PHI is as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

A patient/SDM has the right to challenge the accuracy of their PHI and to request amendment or correction if they feel their PHI is inaccurate or incomplete.

St Joseph's meets this requirement by implementing the following procedure:
- Patient Requests to Amend Personal Health Information

Principle 7 - Ensuring Safeguards for PHI
St Joseph's is responsible to put reasonable security measures in place to protect PHI against such risks as loss, theft, unauthorized access, copying, modification, use or disclosure or unsecure disposal, regardless of the format in which the PHI is held and appropriate to the sensitivity of the information.

St Joseph's meets this requirement by implementing the following policies and processes:
- Security of Confidential Information and Information Technology Systems
- Acceptable Use of Information Technology Resources
- Electronic Mail (Email) Use
- Remote Access to Computer Network Resources

Principle 8 - Openness
St Joseph's is responsible to make information about its policies and practices relating to its management of PHI readily available. Information includes:
- contact information for Patient Relations, Privacy and Risk where concerns or inquiries can be forwarded;
- the means by which patients can gain access to their PHI held by St Joseph's;
- a description of the type of PHI held by St Joseph's, including a general account of its use;

St Joseph's is legally responsible (PHIPA) to notify a patient/SDM if their PHI has been lost, stolen, accessed without authority or disposed in an unsecure manner and to be open and honest about the incident.

St Joseph's meets this requirement by implementing the following policies and processes:
- Breach of Patient Privacy
- Posted notices informing patients/SDMs about the purpose for the collection, use and disclosure of their PHI
- Information on the St Joseph's Privacy Internet site for patients/SDMs including a public-friendly version of this Privacy policy

Principle 9 - Patient Access to PHI
A patient/SDM has the right to request access to their PHI in St Joseph's custody and control. St Joseph's grants access to that PHI, except in limited situations outlined by PHIPA and is responsible to respond to a patient's/SDM's request within the timeline set by PHIPA. St Joseph's establishes fees for access on a cost recovery basis.

St Joseph's meets this requirement by implementing the following policies and processes:
- Access and Disclosure of Personal Health Information

Principle 10 - Challenging Compliance with St Joseph's Privacy Policies and Practices
A patient/SDM has the right to challenge St Joseph's compliance with PHIPA and this policy. St Joseph's also proactively monitors for compliance, e.g. auditing of electronic records systems.

St Joseph's investigates all complaints and suspected breaches of privacy or confidentiality. If a complaint or suspected breach is found to be justified, the organization takes appropriate measures, including, if necessary, amending policies and practices and/or disciplinary action up to and including termination of employment/contract or loss of appointment or affiliation with the organization.

St Joseph's meets this requirement by implementing the following policy:
- Breach of Patient Privacy

DEFINITIONS

Affiliates – Individuals who are not employed by the organization but perform specific tasks at or for the organization, including appointed professionals (e.g., physicians, dentists), students, volunteers, researchers, contractors, or contracted staff who may be members of a third-party contract or under direct contract to the organization, and individuals working at the organization, but funded through an external source (e.g., research employees funded by Western).

Health Information Custodian - Defined in Section 3. (1) of the Personal Health Information Protection Act, 2004 as a person or organization who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties.

Personal health information (PHI) - "As defined by the Personal Health Information Protection Act, 2004 (PHIPA) "…means identifying information about an individual in oral or recorded form, if the information,

a. relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
b. relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
c. is a plan of service within the meaning of the Home Care and Community Services Act, 1994 for the individual,
d. relates to payments or eligibility for health care, or eligibility in coverage for health care, in respect of the individual,
e. relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
f. is the individual's health number, or
g. identifies an individual's substitute decision-maker.""

Substitute Decision-Maker (SDM) – As defined by the Health Care Consent Act, 1996 (HCCA) is a person who is authorized to give or refuse consent to a treatment on behalf of a person who is incapable. The SDM must be capable, willing and available. The SDM must make a decision that is consistent with the patient/client/resident's previously expressed wishes and values. In the absence of previously expressed wishes the SDM must follow the principle of best interest. If a person is incapable with respect to a treatment, consent may be given or refused on their behalf by a person described in one of the following:

1. The incapable person's guardian of the person, if the guardian has authority to give or refuse consent to the treatment.
2. The incapable person's attorney for personal care, if the power of attorney confers authority to give or refuse consent to the treatment.
3. The incapable person's representative appointed by the Board under section 33, if the representative has authority to give or refuse consent to the treatment.
4. The incapable person's spouse or partner.
5. A child or parent of the incapable person, or a children's aid society or other person who is lawfully entitled to give or refuse consent to the treatment in the place of the parent. This paragraph does not include a parent who has only a right of access. If a children's aid society or other person is lawfully entitled to give or refuse consent to the treatment in the place of the parent, this paragraph does not include the parent.
6. A parent of the incapable person who has only a right of access.
7. A brother or sister of the incapable person.
8. Any other relative of the incapable person.
9. If two or more persons who are described above and who meet the requirements disagree about whether to give or refuse consent, and if their claims rank ahead of all others, the Public Guardian and Trustee (PGT) shall make the decision in their stead.
10. If no person described above meets the requirements, the PGT shall make the decision

REFERENCES

Related Corporate Policies

Acceptable Use of Information Technology Resources
Access and Disclosure of Personal Health Information
Addressing Requests from Patients Who Wish to be Anonymous
Breach of Patient Privacy
Confidentiality
Corporate Procurement of Consulting Services
Corporate Procurement of Goods and Non-Consulting Services
Disclosure of Patient Information, Samples and/or Belongings to Law Enforcement Agents
Electronic Mail (Email) Use
Patient Requests to Amend Personal Health Information
Patient Requests to Restrict the Use and Disclosure of Personal Health Information
Records Retention and Destruction
Remote Access to Computer Network Resources
Security of Confidential Information and Information Technology Systems
Use of Personal Health Information for Research, Education and Quality Assurance

Legislation

Government of Ontario (2004) Personal Health Information Protection Act, 2004

Other Resources
St. Joseph's – Privacy Intranet Site
St. Joseph's – Public-friendly version of this Privacy policy