



Privacy, Confidentiality and Security of Information

Background and Purpose

St. Mary's General Hospital is responsible for ensuring the privacy and protection of personal and health information of its patients and employees.

These responsibilities stem from the Public Hospitals Act which directs the disclosure of personal and health information. In anticipation of Ontario health privacy legislation, St. Mary's General Hospital intends to self-regulate to the fullest extent possible, on the basis of Schedule 1 to the Personal Information Protection and Electronic Documents Act PIPEDA.

The policies stipulated herein, are to be used to create and maintain a suitable privacy and security program that allows the hospital to meet its responsibilities.

Scope

St. Mary's General Hospital collects personal information for the purposes of:

- Direct patient care
- Administration and management of the hospital " Research, teaching and statistics " To comply with legal and regulatory requirements

The Privacy, Confidentiality and Security Program and enclosed policies applies to:

- All personal, health, financial, corporate and human resource information in its possession or custody, including information that has been transferred to a third party for processing. St. Mary's General Hospital will use contractual or other means to provide a comparable level of protection while the information is being processed by a third party. ALL formats that can be
- shared: oral, written, and electronic in photograph, on film, or by other means are included.
- All hospital employees or staff. This includes all full- and part-time employees, contractors, consultants, temporaries, student assistants, volunteers, and retired annuitants.

- All 3rd party individuals associated hospital operations: this includes all vendors and other users including those affiliated with third parties who access St. Mary's technology resources due to their job responsibilities.
- All hospital assets deemed as sensitive, confidential, or private.

Privacy and Security Program Goals

It is the intent of St. Mary's General Hospital that the enclosed policies are used to:

3.1 Develop a Privacy, Confidentiality and Security Program based on due diligence and industry best practices that mitigate relevant risks. Risks are based on legislative, malicious and non-malicious exposures.

3.2 Assign a Corporate Privacy Team to develop, implement and maintain the corporate Privacy, Confidentiality and Security Program.

3.3 Develop reasonable standards, guidelines, and implementation procedures that ensure day-to-day activities adhere to the Privacy, Confidentiality and Security Program, including

- a) procedures to protect personal information;
- b) procedures to receive and respond to complaints and inquiries;
- c) training staff and communicating to staff St. Mary's General Hospital's policies and procedures;
- d) developing information to explain policies and procedures

3.4 Ensure that the Privacy, Confidentiality and Security Program policies is reflective of the Mission of St. Mary's General Hospital.

3.5 Implement and integrate the Privacy, Confidentiality and Security Program into day-to-day departmental operations

3.6 Create an ongoing Privacy, Confidentiality and Security Program maintenance and update plan.

Information Privacy Policy

It is the Policy of St. Mary's General Hospital that:

4.1 A bond of trust between clients and care providers be created and maintained such that personal and health information will be kept private, confidential and secure.

4.2 All personal and health information is available for access on a strict need to know basis to authorized personnel.

4.3 Information pertaining to the organization such as financial, corporate and human resource information is also confidential, and should remain so.

4.4 All staff and volunteers are bound by the Hospital Ethics and Confidentiality Policy to protect the privacy and confidentiality of information.

4.5 All personal and Health information is collected, used, disclosed, retained and protected as stipulated by the CSA Model Code:

4.5.1 Accountability

St. Mary's General Hospital is responsible for personal and health information under its control and has designated an individual, the Corporate Privacy Officer who is accountable for St. Mary's compliance with the following principles. In addition, other individuals within St. Mary's General Hospital may be delegated to action on behalf of the designated individual.

4.5.2 Identifying the Purposes for the Collection of Personal or Health Information

The purpose for the collection of personal or health information will be identified at or before the collection of such data.

4.5.3. Consent for the collection, Use and Disclosure of Personal or Health Information

The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when required for the immediate treatment or delivery of care or by law.

4.5.4 Limiting Collection of Personal or Health Information The collection of personal and health information will be limited to that which is necessary for the purpose identified.

4.5.5 Limiting Use, Disclosure and Retention of Personal or Health Information Health Information collected for the care of the patient shall only be used by those who require the information to deliver care, or for management decision-making. Personal information will 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. Information will be retained only as long as necessary for the fulfillment of those purposes, or as required by law.

Ensuring Accuracy of Personal or Health Information Personal Information will be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

Ensuring Safeguards for Personal or Health Information Personal and Health Information shall be protected by security safeguards appropriate to the sensitivity of the information.

Openness about Personal and Health Information Policies and Practices Specific information will be made available to individuals concerning the policies and practices related to the management of personal and health information.

Individual Access to their own Personal or Health Information Upon request, an individual will be informed of the existence, use and disclosure his personal, or health information and will be given access to that information. An individual will be allowed to challenge the accuracy and completeness of the information and have it amended as appropriate

Challenging Compliance with St. Mary's Privacy, Confidentiality, and Security of Information Policies and Practices An individual will be able to address a challenge concerning compliance with the above principles to the Corporate Privacy Officer.

Information and Asset Protection Policy

It is the Policy of SMGH that:

- Access to information is restricted to only those accesses required to perform one's official duties as defined in the job description. These restrictions are based upon the least privileges, and "need to know" required for providing or managing patient care.
- Reasonable administrative, technical and physical safeguards are implemented to ensure the accuracy, and completeness of information, and processing methods.
- Reasonable administrative, technical and physical safeguards are implemented to protect the availability and integrity of information, and associated
- assets.
- Information and assets shall be available for access in a reasonable timeframe to authorized individuals.
- Controls and safeguards will be based upon industry best practice and standards: ISO/IEC 17799:2000 and the RCMP TSSIT

Responsibility and Accountability for the Privacy and Security Program

The development, implementation and maintenance of the hospitals program require that a central point of contact be established. The hospital has appointed a Privacy Team to be responsible and accountable for the Privacy, Confidentiality, and Security Program. Specifically the Team shall:

- Develop standards and guidelines for the privacy and security program that reflect the privacy and security goals of the hospital as well as meet the policies developed herein.
- Assist departments to develop implementation procedures and practices that allow St. Mary's General Hospital to meet policy requirements.
- Ensure appropriate training and education is provided across organization to achieve the goals and intention of the policies.
- Revisit and update security program in light of change control and new threats/exposures.
- Conduct periodic auditing to establish adherence to policies and standards

Enforcement of the Privacy and Security Program

All employees and persons acting on behalf of St. Mary's General Hospital are responsible and shall be held accountable for the privacy and protection of hospital information and assets that are under their direct custody or control. Failure to comply with the provisions of this policy may result in disciplinary measures leading up to and including dismissal or contract termination.

Unauthorized access of information or assets by any individual may result in criminal prosecution.