CORPORATE
MMI004

Policy:	Confidentiality	
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: 2004-11-01	**Reviewed Date:** 2024-08-27	**Revised Date:** 2022-05-25

This policy applies to:
or

- ☒ St. Joseph's Health Care London
- ☐ 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) has a legal and ethical responsibility to protect the privacy of patients/residents/clients, their families, and staff/affiliates, and ensure that confidentiality is maintained.

St. Joseph's considers the following types of information to be confidential:

- Identifiable personal information and personal health information regarding patients/clients (hereafter referred to as "patients") and their families;
- Identifiable personal information, personal health information, certain employment information and compensation information regarding staff and affiliates; and
- Information regarding the confidential business information of the organization, which is not publicly disclosed by the organization.

This policy applies whether this information is verbal, written, electronic, or in any other format. Audits of electronic systems are performed to determine compliance.

In addition to standards of confidentiality, which govern Regulated Health Professionals, staff and affiliates are bound by the organization's responsibility to maintain confidentiality. The organization expects staff/affiliates to keep information, which they may learn or have access to because of their employment/affiliation, in the strictest confidence. It is the responsibility of every staff/affiliate:

- To become familiar with and follow the organization's policies and procedures regarding the collection, use, disclosure, storage, security and destruction of confidential information (See References).
- To collect, access, and use confidential information only as authorized and required to provide care or perform their assigned duties.
- To safeguard confidential information to which they have access, or to which they come in contact, against such risks as loss, theft, unauthorized access or disclosure and unsecure disposal.
- To divulge, copy, transmit, or release confidential information only as authorized and needed to provide care or perform their duties.
- To safeguard passwords and/or any other user codes that access computer systems and programs.
- To identify confidential information as such when mailing or sending e-mails or fax transmissions and to provide directions to the recipient if they receive a transmission in error. (Refer to Electronic (E-Mail) Use Policy and Faxing Guidelines).
- To discuss confidential information only with those who require this information to provide care or perform their duties and make every effort to discuss confidential information out of range of others who should not have access to this information.

- To continue to respect and maintain the terms of the Confidentiality Agreement after an individual's employment/affiliation with the organization ends.
- To participate in the organization's Privacy and Confidentiality education program, review this policy, and sign a Confidentiality Agreement before commencing work or the provision of service at St. Joseph's as a condition of employment/appointment/ contract/association for staff/affiliates at St. Joseph's.
- To report to their Leader suspected breaches of confidentiality, or practices within the organization that compromise confidential information. If the Leader is the individual suspected of the breach, staff/affiliates may contact Patients Relations, Privacy and Risk or Human Resources/Chief of Service.

Misuse, failure to safeguard, or the disclosure of confidential information without appropriate approvals may be cause for disciplinary action up to and including termination of employment/contract or loss of appointment or affiliation with the organization.

PROCEDURE

1. General

1.1. Leaders must review any department specific information or procedures related to confidentiality with new staff and affiliates.

1.2. Staff/affiliates may consult their Leader, Professional Practice Leader, Patient Relations, Privacy and Risk or Human Resources regarding confidentiality issues or inquiries.

2. Confidentiality Agreement

2.1. Confirmation of the completion of the educational program and the signed Confidentiality Agreement will be kept on the individual's file in:

2.1.1 Human Resources for staff.

2.1.2 Medical Affairs Office for physicians, residents, medical students, dentists, and midwives, secretaries who are privately employed by physicians, Medical Department Administrative Officers.

2.1.3 Volunteer Services for volunteers.

2.1.4 Offices of Program/ Leaders under whose supervision contract staff, vendors, or consultants are working (i.e., any individual employed by third-party organizations who are performing work in the organization on a temporary basis).

2.1.5 Student Affairs for non-medical students.

2.1.6 It is the responsibility of Professional Practice Leaders to stipulate in Education Affiliation Agreements with education institutions, the obligation to ensure that students and faculty abide by the organization's standards of confidentiality.

2.1.7 Patient Relations, Privacy and Risk for Lawson affiliates, including students and non-hospital employees.

3. Investigating Alleged Breaches of Confidentiality

It is the responsibility of Patient Relations, Privacy and Risk in conjunction with leaders, and potentially Human Resources to investigate alleged breaches of confidentiality.

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).

Confidential Business Information of the Organization – Information regarding the organization's business, which is not subject to public disclosure under Freedom of Information and Protection of Privacy Act (FIPPA), including, but not limited to:

- Information exchanged in confidence with the Government of Ontario or another government or agency,
- Third party information as described in FIPPA 1990, c. F. 31 s. 17(1),
- Information provided in confidence to, or records prepared with the expectation of confidentiality by a hospital committee to assess or evaluate the quality of health care and directly related programs and services provided by a hospital, if the assessment or evaluation is for the purpose of improving that care and the programs and services,
- Information exchanged with or provided to legal counsel in the process of seeking advice or legal opinion,
- Negotiations related to labour relation matters and settlements,
- Negotiations that give rise to employment or employment contracts,
- Legal matters that involve the organization that are not public knowledge,

- Plans relating to the management of personnel or the administration of an institution that have not yet been put into operation or made public,
- Information related to intellectual property held by the organization (e.g. information directly included in patents or other intellectual property applications, prior to publication of those patents or applications in public format),
- Information related to the organization's information technology security and access to systems, including:
    - Information leading to improper access to the organization's computing resources, both internal and external to the hospital network (e.g., "guest" access to systems, remote access credentials),
    - Hardware and software vendor names for products which may be vulnerable to external access attacks, or products that are part of our security infrastructure.

Confidentiality – The obligation upon an organization or person to protect information that has been entrusted to its care for a specific purpose and to ensure that information is only accessible to those authorized to have access.

Personal Health Information – "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.""

Personal Information – "As defined by the Freedom of Information and Protection of Privacy Act (FIPPA) "means recorded information about an identifiable individual, including:

a. information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
b. information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
c. any identifying number, symbol or other particular assigned to the individual,
d. the address, telephone number, fingerprints or blood type of the individual,
e. the personal opinions or views of the individual except where they relate to another individual,
f. correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,
g. the views or opinions of another individual about the individual, and
h. the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;"

"Personal information does not include information about an individual who has been dead for more than thirty years."
"Personal information does not include the name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity.""

Staff – An individual who is hired and paid by the organization.

REFERENCES

Related Corporate Policies

Access to and Disclosure of Personal Health Information
Breach of Patient Privacy
Electronic (E-Mail) Use
Privacy
Security of Confidential Information and Information Technology Systems

Legislation

Government of Canada (2000) Personal Information Protection and Electronic Documents Act, 2000
Government of Ontario (1990) Freedom of Information and Protection of Privacy Act (FIPPA), 1990
Government of Ontario (2004) Personal Health Information Protection Act, 2004
Government of Ontario (1990) Public Hospitals Act, 1990 (as amended)

Government of Ontario (1991) Regulated Health Professional Act, 1991 (as amended)

Other Resources

College of Nurses of Ontario, Standards of Practice – Confidentiality
College of Physicians and Surgeons of Ontario – Confidentiality of Personal Health information
St. Joseph's – Guidelines for Faxing Confidential Information
St. Joseph's – Waste Management Manual