Middlesex Hospital Alliance Strathroy Site ☒ Four Counties Site ☒	Policy ☒ Procedure ☐	Standard ☐
Subject: Breach of Privacy Policy		
Owner: Privacy Office	**Reviewer(s):** Health records Manager Human Resources	**Approver:** VP Finance / CFO & CIO
Cross Reference:		

BACKGROUND:

It is the responsibility of all employees and affiliates of Four Counties Health Services and Strathroy Middlesex General Hospital, hereafter referred to as the Middlesex Hospital Alliance (MHA) to comply with their ethical, professional, employment and legal obligations to maintain the confidentiality and security of personal health information (PHI) entrusted to them.

POLICY or STANDARD or MEDICAL DIRECTIVE STATEMENT:

The Middlesex Hospital Alliance (MHA) as a health information custodian under the Personal Health Information Protection Act (PHIPA) and an organization under the Freedom of Information and Protection of Privacy Act (FIPPA) is responsible and accountable for the privacy and security of:

- Personal health information (PHI) of all patients registered for visits to the organization regardless of the purpose of the visit
- Personal information (PI) we collect from any individual (e.g. staff, visitor, vendor).

A privacy breach occurs whenever PHI or PI is:

- Lost or stolen, or
- Accessed, disclosed, copied or modified without authority, or
- Disposed of in an unsecure or unauthorized manner.

A privacy breach may occur via verbal or written communication, by phone, e-mail, fax, electronic means or any other medium.

PROCEDURE:

By law, MHA must notify an individual, patient, or an incapable patient's Substitute Decision Maker (SDM), if there has been a breach of their privacy related to their PHI/PI.

Staff and affiliates must:

- Comply with their obligations and all corporate policies related to confidentiality, privacy and security of confidential information.
- Protect and secure PHI and PI to reduce the risk of a breach.
- Immediately notify their leader and the Privacy Office, if they become aware of a potential or suspected privacy breach or if they become aware of a complaint about an alleged breach.
- Participate in the investigation and management of a breach, with Union representation as applicable.

Leaders must:

- Notify the Privacy Office if they become aware of a potential or suspected privacy breach.
- Collaborate with the Privacy Office to promptly contain and investigate the breach.
- Collaborate with the Privacy Office to:

  - Notify the affected individuals.

  - Review the information obtained as part of the breach investigation and put measures in place to reduce the risk of recurrence.

The Privacy Office must:

- Notify the affected leader if made aware of a potential or suspected privacy breach.
- Report high risk privacy breaches to the Information and Privacy Commissioner/Ontario (IPC) and work with the IPC to ensure the organization has met its legal obligations under PHIPA and FIPPA.

Breach of privacy may be cause for disciplinary action, up to and including termination of employment/contract or loss of appointment or affiliation with the organization. In addition, a privacy breach can result in:

- Loss of public trust;
- Legal action by a patient or individual;
- A complaint to the organization and/or to the Information and Privacy Commissioner (IPC);
- An Order by the IPC (requires the organization to take certain actions to prevent recurrence of a similar breach and sets a standard for all Ontario Health Information Custodians; Orders are published and result in media attention);
- Fines and penalties set out in PHIPA.

DEFINITIONS

Affiliates – Individuals who are associated with the hospital, performing specific tasks for the hospital, including the following:

- Professional with Hospital Privileges - Refers to those professionals formally affiliated with the hospital through the process of review of credentials and approval of privileges (e.g. Physicians)
- Students - Individuals gaining practical/clinical experience in the hospital whether directly affiliated with the hospital or not
- Volunteers - Individuals who perform recognized functions within the hospital on a volunteer basis

- Contractor - Individuals who are performing work in the hospital on a temporary basis. These individuals may be under direct contract to the hospital or may be members of a third party contract (e.g. construction workers, landscape/snow removal workers, agency nurses).
- Individuals working at the MHA, but funded through an external source.

Leader – Operational leader, director, coordinator, professional practice leader, union leader, chiefs, senior leader.

Personal Health Information – As defined by the Personal Health Information Protection Act (PHIPA), identifying information about an individual, in oral or recorded form, if the information:

- Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
- 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,
- Relates to payments or eligibility for health care in respect of the individual,
- 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,
- Is the individual's health number, or
- Identifies an individual's substitute decision-maker.

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

- Information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,
- 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,
- Any identifying number, symbol or other particular assigned to the individual,
- The address, telephone number, fingerprints or blood type of the individual,
- The personal opinions or views of the individual except where they relate to another individual,
- 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 original correspondence,
- The views or opinions of another individual about the individual, and
- 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
- The name, title, contact information or designation of an individual that identifies the individual in a business, professional or official capacity.

Privacy Breach - Actual – an individual's personal health information or personal information (PHI/PI) is lost, stolen, accessed, used, disclosed, copied or modified without authority.

Privacy Breach - Potential – an individual's personal health information or personal information (PHI/PI) is at high risk of being lost, stolen, accessed, used, disclosed, copied or modified without authority.

Privacy Breach - Suspected – allegations or concerns that an individual's personal health information or personal information (PHI/PI) has been lost, stolen, accessed, used, disclosed, copied or modified without authority.

REFERENCE:

Legislation

Personal Health Information Protection Act, 2004
Freedom of Information and Protection of Privacy Act
Public Hospitals Act 1990 (as amended)
Regulated Health Professions Act 1991 (as amended)