PATIENT PRIVACY POLICY

What is Personal Health Information?

Personal health information (PHI) means identifying information about an individual relating to their physical or mental health (including medical history), the provision of health care to the individual, payments for eligibility for health care organ and tissue donation and health number.

Purpose

The Marathon Family Health Team is dedicated to quality patient care and improving the health status of our communities. The Marathon Family Health Team is committed to protecting individual privacy and the confidentiality and security of the records of personal health information (PHI) it holds.

Protecting your privacy and the confidentiality of your personal health information has always been an important aspect of the Marathon Family Health Team's operations. The appropriate collection, use and disclosure of patient's personal health information are fundamental to our day-to-day operations and to your care.

The Marathon Family Health Team employees, volunteers and other agents are accountable for maintaining confidentiality of all information collected, accessed or disclosed during and after their employment or professional contact. Employees and agents are authorized to use personal health information on a need-to-know basis only. Unauthorized access to personal health information unrelated to the individual's role at the Marathon Family Health Team will be subject to discipline up to and including termination or an impact on or end to the relationship with the Marathon Family Health Team for those who are not employees or other agents.

All personal health information collected, used, accessed or disclosed is protected as referred to in the following interrelated principles.

The 10 Principles of Privacy

The Marathon Family Health Team Privacy Policy reflects our compliance with fair information practices, applicable laws and standards of practice.

1. **Accountability for Personal Information**

   We take our commitment to securing patient privacy very seriously. Each physician and employee associated with the Clinic is responsible for the personal information under their possession including information that has been transferred to a third-party for processing.

   Employees are informed about the importance of privacy and receive information periodically to update them about our Privacy Policy and related issues.

   The Executive Director oversees compliance with the policy, related procedures and legislation. The identity and contact information of this person is made known to the public under Principle 10.

2. **Identifying Purposes for Collecting Personal Information**

   We ask you for information to establish a relationship and serve your medical needs. We obtain most of our information about you directly from you, or from other health practitioners whom you have seen and authorized to disclose to us. You are entitled to know how we use your information and this is described in the Privacy Statement posted at the Marathon Family Health Team Clinic.

   Personal information related to patients is collected, used, disclosed and retained for:

   - Direct patient care
   - Administration of the health care system
   - Risk management
   - Quality improvement and to improve the services provided by the Marathon Family Health Team
   - Research, teaching, statistics, and
   - To meet legal and regulatory requirements

3. **Consent for Collection, Use and Disclosure of Personal Health Information**

   You have the right to determine how your personal health information (PHI) is used and disclosed. For most health care purposes, your consent is implied as a result of your consent to treatment, however, in all circumstances express consent must be written.

   Your written Consent will be forwarded to the Privacy Officer who will document the request in the patient's medical record and notify appropriate Health care providers and their supporting staff.

Patients who have withdrawn consent to disclose PHI must sign and date the Consent to Withdrawal Form. It is understood that the consent directive applies only to the PHI which the patient has already provided, and not to PHI which the patient might provide in the future: The Personal Health Information Protection Act (PHIPA) permits certain collections, uses, and disclosures of the PHI, despite the consent directive; healthcare providers may override the consent directive in certain circumstances, such as emergencies; and the consent directive may result in delays in receiving health care, reduced quality of care due to healthcare provider's lacking complete information about the patient, and healthcare provider's refusal to offer non-emergency care. Your written Consent to Withdrawal Form will be forwarded to the Privacy Officer who will document the request in patient's medical records and notify appropriate Health care providers and their supporting staff.

4. **Limiting Collection of Personal Health Information**

We collect information by fair and lawful means and collect only that information which may be necessary for purposes related to the provision of your medical care.

5. **Limiting Use, Disclosure and Retention**

Personal Health Information will not be used or disclosed for purposes other than those for which it was collected, except with the consent from the individual or as permitted or required by law, including the Personal Health Information Protection Act (PHIPA).

Under no circumstances do we sell patient lists or other personal information to third parties. There are some types of disclosure of your personal health information that may occur as part of the Clinic fulfilling its routine obligations and/or practice management. This includes consultants and suppliers to the Clinic, on the understanding that they abide by our Patient Privacy Policy, and only to the extent necessary to allow them to provide business services or support to this Clinic.

We will retain your information only for the time it is required for the purposes we describe and once your personal information is no longer required, it will be destroyed.

Patients may be required to sign and date a "Consent to Disclose PHI" form and pay a fee based on current OMA rates prior to release of information.

6. **Accuracy of Personal Health Information**

   Personal information will be as accurate, complete and up-to-date as possible and as is necessary for the purposes for which it is intended.

   While we will do our best to base our decisions on accurate information, we rely on you to disclose all material information and to inform us of any relevant changes.

7. **Safeguards: Protecting Your Information**

   The Marathon Family Health Team has security safeguards in place to protect PHI against loss, theft, unauthorized access, disclosure, copying, use or modification regardless of the format in which it is held. Care will be used in the disposal or destruction of PHI to prevent unauthorized persons gaining access to the information.

   These safeguards are administrative (policies and procedures, including signing of confidentiality oath and training); technical (secure electronic systems) and physical (locked doors and cabinets).

   Access to personal information is authorized only for the physicians and employees associated with the Clinic, and other agents who require access in the performance of their duties, and to those otherwise authorized by law.

8. **Openness: Keeping You Informed about Privacy Policy**

   The Marathon Family Health Team makes available to its patients and clients, information regarding the policies and practices relating to the management of personal health information in a format that is generally understandable.

   If you have any additional questions or concerns about privacy, we invite you to contact us by phone, in person or by letter and we will address your concerns to the best of our ability.

9. **Individual Access and Correction**

   With limited exceptions, we will give you access to the information we retain about you within a reasonable time, upon presentation of a written request and satisfactory identification.

   We may charge you a fee for this service and if so, we will give you notice in advance of processing your request.

If you find errors of fact in your personal health information, please notify us as soon as possible we will respond to these requests for correction in accordance with the Personal Health Information Protection Act (PHIPA).

We are not required to correct information relating to clinical observations or opinions made in good faith. You have a right to append a short statement of disagreement to your medical record if we refuse to make a requested change.

If we deny your request for access to your personal information, we will advise you in writing of the reason for the refusal and you may then challenge our decision.

10. **Challenging Compliance with the Privacy Policy**

The Executive Director investigates all complaints.

We encourage you to contact us with any questions or concerns you might have about your privacy or our Patient Privacy Policy. We will investigate and respond to your concerns about any aspect of our handling of your information.

If a complaint is found to be justified, appropriate measures will be taken, including amending our policies and practices if necessary.

In most cases, an issue is resolved simply by telling us about it and discussing it.

You can reach us at:

Executive Director
Marathon Family Health Team,
22 Peninsula Road, PO Box 399
Marathon, Ontario
P0T 2E0
Telephone # 807-229-3243

If, after contacting us, you feel that your concerns have not been addressed to your satisfaction, you have the right to complain to the Information and Privacy Commissioner/Ontario. The Privacy Commissioner can be reached at:

2 Bloor Street East, Suite 1400
Toronto, Ontario
M4W 1A8
Telephone #1-800-387-0073, 1-416-325-9195 (fax)

PROCEDURE:

Personal Health Information is "identifying" information about an individual's health or health care history. It includes:

- The individual's physical or mental health, including family history
- The provision of health care to the individual
- Long-term care services
- The individual's health card number
- Blood or body part donations
- Payment of eligibility for health care
- The identity of a health care provider or a substitute decision maker for the individual.

A health information custodian (HIC) is an individual or organization that, as a result of their power or duties, has custody or control of personal health information.

Examples of health information custodians include:

- Health care practitioners (physicians, nurses, social workers, dietitians, etc.)
- Hospitals, including psychiatric facilities
- Pharmacies
- Laboratories
- Nursing homes, retirement homes and long term care facilities
- Community Care Access Centers
- Ambulance services
- Ministry of Health and Long Term Care

The **Circle of Care** is not a defined term under PHIPA. It is a term of reference used to describe health information custodians and their authorized agents who are permitted to rely on an individual's implied consent when collecting, using, disclosing or handling personal health information for the purpose of providing direct health care.

In a Family Health Team, the circle of care can include:

- Physicians
- Nurses
- Specialists or other health care providers
- Health care professionals selected by the patient (e.g. pharmacist)

Consent

Express consent may be given verbally, in writing or by electronic means (if it is provided verbally, it should be documented in the patient's health record).

Express consent is always required in certain circumstances.

- E.g., for disclosure of personal health information to an individual or organization that is not a health information custodian and is outside the circle of care (e.g. an insurance company).
- When information is disclosed by one custodian to another for a purpose other than providing or assisting in providing health care.
- When a health information custodian provides information other than name and address for marketing, fundraising or research purposes.

Implied consent permits a health information custodian to infer from the surrounding circumstances that an individual would reasonably agree to the collection, use of and disclosure of his/her personal health information.

Under PHIPA, the Marathon Family Health Team also implies consent when it is provided personal health information either by the patient or client, that person's substitute decision-maker, or another health practitioner.

What are the implications of PHIPA for Marathon Family Health Team?

1. Unless the patient has withdrawn implied consent under PHIPA, personal health information may be sent to a specialist, and returned to the primary care provider without patient consent. This is considered to be transfer of information within the circle of care and consistent with good clinical care.

2. The Marathon Family Health Team must request and receive express consent before providing personal health information to anyone outside the circle of care – e.g. insurance companies, employers – unless PHIPA specifically permits the information to be used by the Marathon Family Health Team or disclosed outside the Marathon Family Health Team without consent.

3. The Marathon Family Health Team staff must not provide personal health information to anyone other than the patient without express consent of the patient. This includes the provision of information to family members, unless a family member is acting as a substitute decision-maker for the patient or under other limited circumstances under PHIPA.

4. Staff must use their best efforts to protect patient confidentiality. Patient records should be protected, computer screens should not be visible to patients or visitors, conversations should be kept private.

5. Staff must not access patient records unless required for treatment or care purposes. Unauthorized access, outside the employee's role at the Marathon Family Health Team, or without patient consent where PHIPA requires it, is cause for disciplinary action, up to and including dismissal.

RELEVANT LINK(S):

PHIPA – Personal Health Information Protection Act, 2004

Withdrawal of Consent

I, _____, wish to withdraw my consent to any further use or disclosure by the **Marathon Family Health Team** of my personal health information to:

_____

(Insert name of organization / survey / research project withdrawing from)

OR

I wish to put the noted conditions on any further use or disclosure of my personal health information:

Patient Name:

_____

(Please Print in Block Letters)

Patient Signature: _____ Date: _____

Witness: _____ Date: _____

Annual Privacy & Confidentiality Pledge

For Staff/Contractors/Physicians/Students/Board Members/Vendors/Volunteers

I pledge to keep private and confidential any information obtained during the performance of my duties at the Marathon Family Health Team.

I understand that private and confidential information includes information relating to:

- Patients (and patient information would include health records (paper or electronic), health information in any format, conversations, registration information, financial history, the fact that someone is, has been or may become a patient of Marathon Family Health Team, the name of a substitute decision maker, etc.);
- Marathon Family Health Team employees, physicians, students, volunteers, contractors or vendors (such as employee records, disciplinary action, performance reviews, quality reports, etc.);
- Marathon Family Health Team business information (such as contracts, financial information, memos, peer review information, etc.).

I agree that I have read and agree to follow the Marathon Family Health Team Patient Privacy Policy.

If I need help understanding this policy, I will ask the Executive Director and Privacy Officer of the Marathon Family Health Team.

I also understand and agree that:

- I am only allowed to collect (including to receive, look at, access, ask for, view, copy, record, print, read, listen), use and disclose confidential information on a "need-to-know basis" only, and even then only the minimum amount required, **as required for my role** or **as I have been authorized to do in writing** or **as required by law**.
- I will not communicate private or confidential information either within or outside Marathon Family Health Team, except to persons authorized to receive such information and only for the purposes of performing my duties.
- I will not collect, use or disclose the private or confidential information of family, friends or co-workers or any other individual, unless they are under my direct care or I am authorized as part of my official duties at the Marathon Family Health Team and not for my own purposes.

Annual Privacy & Confidentiality Pledge (Cont'd)

- I will only access my own health information in the custody or control of Marathon Family Health Team through the method approved for the public in the Marathon Family Health Team Patient Privacy Policy.
- If I am a patient's substitute decision-maker, I will only access the patient's health information through the method approved for the public in the Marathon Family Health Team Patient Privacy Policy.
- I am not allowed to engage in self-study (such as learning how to document or learning about our patients and the services we offer them or learning how others provide services) with personal health information in the custody or control of the Marathon Family Health Team without written permission from my Supervisor or the Privacy Officer.
- I will not share my passwords to electronic information systems with anyone. I understand I am responsible for protecting those passwords and access to Marathon Family Health Team's systems and records and that I am responsible for all actions performed when the electronic information system has been opened using my password.
- I will access, process and transmit all private or confidential information using only authorized hardware, software, or other authorized equipment. I understand that I may not save private or confidential information on an unencrypted USB key or other portable device.
- I shall not remove private or confidential information from Marathon Family Health Team premises (including taking it home to work on) except as authorized by my Supervisor or Privacy Officer. If authorized, I shall securely store the information and ensure it is in my custody and control at all times.
- I will not alter, destroy, copy or interfere with confidential information, except with authorization and in accordance with Marathon Family Health Team policies and procedures.
- I shall immediately report all incidents involving loss, theft or unauthorized access to private or confidential information to my Supervisor and to the Marathon Family Health Team's Privacy Officer.

I understand that the Marathon Family Health Team conducts regular audits to ensure private or confidential information is protected against unauthorized access, use, disclosure, copying, modification or disposal.

Annual Privacy & Confidentiality Pledge (Cont'd):

I understand that any breach of my duty to maintain privacy or confidentiality may result in corrective action. Such corrective action taken may include retraining, loss of access to systems, suspension, reporting my conduct to the Information and Privacy Commissioner of Ontario or a professional regulatory body or sponsoring agency, school or institution, restriction or revocation of privileges, and up to and including immediate dismissal.

I understand there could also be notification of affected persons.

I understand a privacy breach could also result in me being fined, prosecuted or sued and other consequences.

I understand and agree to abide by the conditions outlined in this pledge, and they will remain in force even if I cease to be employed by or have association with the Marathon Family Health Team.

Print Name & Signature:

_____

Date: _____

BREACH OF PATIENT PRIVACY POLICY

The Marathon Family Health Team (MFHT) as a Health Information Custodian (HIC) under the Personal Health Information Protection Act (PHIPA) 2004 is responsible and accountable for the privacy and security of the personal health information (PHI) under its custody and control.

It is the policy of MFHT that all employees and affiliates will:

- comply with obligations related to privacy and confidentiality
- protect and secure all personal health information (PHI) entrusted to them, to prevent a breach of a patient's privacy
- to act immediately if made aware of an actual or potential privacy breach.
- Participate in the investigation and management of a privacy breach with appropriate representation, as applicable.

Effective October 1st, 2017, the Personal Health Information Protection Act (PHIPA) has been amended to include 7 situations that require notification of privacy breaches to the Information Privacy Commissioner of Ontario.

These are not mutually exclusive; more than one can apply to a single privacy breach. If at least one applies, we have a duty to report. The following is a summary of these situations:

1. Use or disclosure without authority

   Covers situations where the person committing the breach knew or ought to have known that their actions are not permitted either by the act or the responsible custodian. EG: looking at an ex-spouse's medical history for no work related purpose (snooping case). This also includes situations where the unauthorized use or disclosure is not done for personal or malicious motive – i.e. just curious – person is a celebrity and they want to know why they were treated. If the breach was accidental, you generally do not have to notify the Commissioner if they have accidentally accessed the wrong patient record, however, even accidental privacy breaches must be reported if they fall into one of the other categories of breach.

2. Stolen Information

   Someone has stolen paper records, a laptop or other electronic device. Another example would be where patient information is subject to ransomware or other malware attack, or if information has been seized through use of a portable storage device. If the information was properly encrypted, you do not need to report.

3. Further use or disclosure without authority after a breach

   Following an initial privacy breach, you might become aware that the information was or will be further used or disclosed without authority. EG: Staff inadvertently sent a fax containing patient information to the wrong person. Although the person returned the fax to you, you learn that the person has kept a copy and is threatening to make the information public. Or, you learn that an employee has wrongfully accessed patient information and subsequently used this information to market products or services in order to commit fraud (EG: healthcare or insurance fraud).

4. Pattern of Similar Breaches

   If a privacy breach is accidental or insignificant by itself, it must be reported if it is part of a pattern of similar breaches. Such a pattern may reflect system issues that need to be addressed, such as inadequate training or procedures. Letters generated to patients regularly include information relating to other patients. This mistake is repeated because an automated process for generating letters has been malfunctioning for some time.

5. Disciplinary action against a college member

   A duty to report an employee or other agent to a health regulatory college also triggers a duty to notify the Commissioner, when:

   - You terminate, suspend or discipline them as a result of the breach
   - They resign and you believe this action is related to the breach

   Or if they have privileges or otherwise are affiliated with you, you must notify if:

   - You revoke, suspend or restrict their privileges or affiliation and you believe as a result of the breach
   - They relinquish or voluntarily restrict their privileges or affiliation and you believe this action is related to the breach.

6. Disciplinary action against a non-college member

   Not all employees or other agents of a health information custodian are members of a college. If an agent is not such a member, you must notify in the same circumstances that would have triggered notification to a college had the agent been a member.

   EG: One of the reception staff has an unpleasant encounter with a patient and posts information about the patient on social media. You suspend the receptionist for a month. Although the receptionist is not a member of a college, the breach must be reported.

7. Significant breach

   Even if none of the above six circumstances apply, you must notify if the breach is significant. In deciding whether a breach is significant, you must consider all the relevant circumstances, including whether;

   - The information is sensitive
   - The breach involves a large volume of information
   - The breach involves many individual's information
   - More than one health care custodian or agent was responsible for the breach

   EG: You are a health care provider who accidentally discloses a patient's mental health assessment to other health care providers on a group email distribution list, rather than just to the patient's physician. This information is highly sensitive and has been disclosed to a number of persons to whom you did not intend to send the information to.

A privacy breach can occur via verbal or written communication, via phone, e-mail, fax or any other medium.

A privacy breach can be actual, or potential. (see definitions of actual, or potential privacy breaches for examples presented further in this document).

Pursuant to (PHIPA 2004, revision October 1, 2017), MFHT must notify a patient, or the patient's Substitute Decision Maker (SDM), if there has been a breach of privacy related to their PHI. It is the responsibility of the Privacy Officer or delegate, to notify the patient or SDM. (Note: the Privacy Officer is the Executive Director)

A 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 as outlined in the Patient Privacy Policy and Annual Confidentiality Pledge signed by all employees and affiliates.

PROCEDURE

MFHT may become aware of a potential or actual privacy breach by:

- Patients, employees or affiliates who believe personal health information has been breached or compromised may complain to the caregiver or the Privacy Officer or delegate,
- A representative from the Information and Privacy Commissioner (IPC) will notify the Privacy Officer or delegate and request a response within a specified period of time, following a patient complaint to the IPC.
- An audit of the organization's electronic medical record system (EMR) or other system containing personal health information has resulted in reason to believe that there may have been an inappropriate access to a patient's personal health information,
- Health Information Custodians(HIC), private homes, businesses or individuals who are not health care providers reporting a potential or actual breach to the Privacy Officer or delegate or their Leader or delegate.
- A secondary breach identified through the initial investigation of another breach.

In accordance with guidelines provided by the Office of the Information and Privacy Commissioner of Ontario, MFHT will take the following steps when made aware of a potential or actual privacy breach.

Step 1: Act Immediately: Contain the Breach and Secure the Personal Health Information

Employees and affiliates, upon learning of a potential or actual privacy breach must notify the Privacy Officer or delegate, immediately.

Depending on the severity and nature/type of the breach:

1. The Privacy Officer or delegate may involve the following individuals as soon as reasonably possible,

   - Board Chair
   - Medical Director
   - Information Management, and/or the Trusted User (if immediate suspension of access is required to further contain the breach)
   - Police if the breach may reasonably be considered to result in significant harm to the patient or third party.
   - Others as deemed necessary.

2. The Privacy Officer or delegate will direct employees and affiliates to immediately contain the breach.

Containing the breach may include:

- Determining whether the breach would allow unauthorized access to any other personal health information and, if so, take any and all steps necessary to contain the breach, e.g. change passwords, or temporarily shut down a system,
- Suspending a users' access to patient care systems or other hospital systems to prevent reoccurrence of the breach. Suspending a user's access will only be done with the authority of Executive Director or designate.
- Notifying the employee(s) involved of the situation, indicating that an investigation is being conducted, and that the Privacy Officer or delegate will be monitoring their access.
- In the case of information that has been mailed or faxed to the wrong recipient retrieving the information by:

    - Obtaining contact information from the recipient,
    - Asking the recipient to place the information in a sealed envelope and place in a secure area,
    - Asking the recipient not to make any copies of the information,
    - Notify the Privacy Officer or delegate who will arrange a courier to retrieve the information, if required.

Step 2: Investigate the Potential/Actual Breach and Evaluate the Risks Associated with the Breach

The Privacy Officer or delegate will conduct an investigation to determine the extent of the breach. Steps that may be taken as part of the investigation include:

- Auditing the electronic medical record (EMR)
- Hard copy health record review
- Interviews with employees, physicians, students, volunteers or affiliates
- Interviews with patients and or SDM

Depending on the severity of the breach, the Privacy Officer or delegate will identify and manage risks associated with the breach, including risk related to:

- Reputation of the organization
- Patient trust
- Media
- Legal
- Collaborate on determining next steps/actions

Outcomes for employee / affiliate:

On completion of the investigation, the Privacy Officer, in collaboration with the Board Chair determines the most appropriate outcome for the employee/affiliate. Possible outcomes include one or more of the following:

- Education
- Verbal warning
- Written warning
- Suspension
- Termination

Factors to consider when determining an outcome include:

- History of work performance or any prior discipline. Note the time lapse between disciplinary infractions and the employee's tendency to respond favorably to discipline
- Years of service
- Employee/affiliate's response to the investigation
- Whether the employee/affiliate understands the concept of privacy and confidentiality and understands the seriousness of the breach

Step 3: Notification

Patient Notification

The Privacy Officer is legally required to notify;

- A patient or an incapable patient's substitute decision maker (SDM), if the patient's information has been breached per the 7 situations described previously.

Notification of a patient/SDM may be done verbally or in writing depending on several factors:

- Availability of patient/SDM, i.e. if the patient is coming to the Clinic in the near future, it may be appropriate for the physician or Privacy Officer to notify the patient in person
- Relationship with the patient, i.e. if the physician or health care provider has an established clinical relationship with the patient, it may be appropriate to notify the patient in person

When applicable, the notification indicates that an employee has received disciplinary action but does not disclose details of the action, e.g. that the staff received a written warning or a suspension. The initial notification does not disclose the name of the employee who committed the breach, but if the patient requests the information, this information is disclosed.

Other Organizations

In the event that an actual or potential breach is identified as involving or potentially involving another organization's employee/user and/or a patient's Personal Health Information, through the electronic medical record (EMR) or other communication venues, the Privacy Officer will immediately:

- Notify the Privacy Officer, or designate of the organization(s) that are affected by the breach.

The Office of the Information Privacy Commission of Ontario (IPC)

The Privacy Officer is responsible to submit a report outlining the breach, the investigation, patient notification and outcome to the Office of the Information Privacy Commissioner of Ontario and work with the Commissioner's staff to ensure that MFHT has met it's legal obligations under PHIPA.

Effective January 1st, 2018, health care custodians will be required to start tracking privacy breach statistics and will be required to provide the Commissioner with an annual report of the previous year's statistics starting in March 2019.

Managing the Risk of Future Breaches

All those involved in managing the breach will review the breach and information obtained as part of the investigation with an aim to take measures to reduce the risk of reoccurrence. These measures may include:

- Changes to policies, procedures or system processes
- Additional education/training for employees and/or affiliates related to personal health information and their accountabilities for confidentiality and the protection of patients privacy rights
- Reviewing and enhancing the programs or department's security of personal health information

DEFINITIONS (for further clarity)

Affiliates: Individuals who are not employed by the organization but perform specific tasks at or for the organization, included appointed professionals (e.g. locum physicians, midwives, dentists), students, volunteers, researchers, contractors or contract employees 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.

Health Information Custodian: Listed person or organization under the Personal Health Information Protection Act such as hospitals and physicians who have custody or control of personal health information as a result of the work they do.

Personal Health Information: Is any identifying information with respect to an individual, whether living or deceased and includes:

- Information concerning the physical or mental health of an individual
- Information concerning any health service provided to the individual
- Information concerning the donation by the individual of any body part or any bodily substance of the individual
- Information derived from the testing or examination of a body part or bodily substance of the individual
- Information that is collected in the course of providing health services to the individual; or
- Information that is collected incidentally to the provision of health services to the individual.

Privacy Breach – Actual – Includes, but is not limited to:

a) Accessing patient personal health information when it is not required to provide or maintain care to a patient or in the performance of duties. For example:

    - Directly accessing the EMR of one self without following the MFHT Patient Privacy Policy.
    - Directly accessing the EMR to book appointments for one self.
    - Accessing the health record of an employee, family member, friend, or anyone for whom you do not have a requirement to view information based on providing care or performing duties
    - Accessing any patient information (e.g. address, date of birth, next of kin, etc.) of an employee, family member, friend, or anyone for whom you do not have a requirement to view information based on providing health care or performing duties

b) Discussing patient information with:

- Another person who is not involved in the direct care of the patient or does not required the information to perform their job functions, or
- Within range of other people in a non-patient area of the Clinic (E.g. discussing information related to patient care with another employee in the waiting area)

c) Failing to ensure the security of patients' PHI, for example:

- Faxing or emailing PHI to the wrong recipient
- Theft of electronic devices containing identifiable patient information

Privacy Breach – Potential – Occurs when an individual's personal health information is at <u>high</u> risk of being accessed, used or disclosed inappropriately by or to individuals or for purposes other than consented to by the patient. A potential privacy breach includes, but is not limited to:

a) Allegations of a privacy breach by a patient or employee/affiliate
b) Concerns related to security of PHI raised by a patient or employee/affiliate
c) Request by a patient for additional security around their PHI (e.g. Lock Box)
d) Leaving patient information in unattended or unsecured locations where it may be accessed by unauthorized persons
e) Leaving access to electronic patient information unattended on an open log-in
f) Storing electronic patient identifiable information on portable information devices or un-secure devices, e.g. hard drives that have not been encrypted
g) Loss of hard copy health record or other identifiable patient information

Substitute Decision Maker (SDM)

A substitute decision maker (SDM) is defined as a person who is:

- At least 16 years of age, unless he/she is the incapable patient's parent
- Capable with respect to the treatment
- Not prohibited by court order or separation agreement from having access to the incapable patient or giving or refusing consent on the incapable patient's behalf
- Available; and
- Willing to assume the responsibility of giving or refusing consent

In descending order of priority, an incapable patient's SDM may be:

i. The incapable patient's **"guardian of the person"**, appointed under the Substitute Decisions Act, 1992, if the guardian has the authority to give or refuse consent to the treatment.
ii. The incapable patient's **"attorney for personal care"**, given under the Substitute Decisions Act, 1992, if the power of attorney confers authority to give or refuse consent to treatment
iii. The incapable patient's **"representative"** appointed by the Consent and Capacity Board, if the representative has authority to give or refuse consent to the treatment
iv. The incapable patient's **spouse or partner**
v. a **child or parent (custodial)** of the incapable patient, or a Children's Aid Society or other person who is lawfully entitled to give or refuse consent to the treatment in place of the parent
vi. a **parent (who has only a right of access)** of the incapable patient
vii. a **brother or sister** of the incapable patient
viii. **any other relative** of the incapable patient
ix. the **Public Guardian and Trustee**

REFERENCES

Personal Health Information Protection Act – PHIPA, 2004 (as amended)

Regulated Health Professionals Act 1991 (as amended)

Privacy Breach Summary Form

Date of privacy breach:

Date reported to Executive Director:

Name of Patient:

Location where breach occurred:

Summary of issue:

Outline of steps taken to resolve this issue:

Summary of conversation with patient regarding this breach:

If employee at fault, summary of conversation with employee, including any discipline taken:

Summary of final resolution:

Recommendations to ensure a similar privacy breach does not occur in the future:

Signature of Executive Director:

Date: