| | | | |
|---|---|---|---|
| **Title:** | **Privacy Policy** | | |
| **Manual:** | Corporate | | |
| **Section:** | Privacy | | |
| **Approval Body:** | Corporate Operations Committee | | |
| **Original Effective Date:** *(mm/dd/yyy)* | 05/08/2003 | **Reviewed Date:** *(mm/dd/yyy)* | 11/01/2016 |
| **Revised Date:** *(month/yyyy)* | 11/01/2016 | **Next Revision Date:** *(month/yyyy)* | 11/01/2019 |
| **Cross References:** | Code of Conduct | | |
| **Key Words:** | Privacy Personal Health Information | | |
| **Developed by:** *(Name & Title)* | **Manager, Privacy & Information Security** | **Owner:** *(Name & Title)* | **Chief Information Officer** |

## POLICY:

All personnel are required to comply with Mackenzie Health's Privacy program as direction in protecting both Mackenzie Health's reputation and preserving individuals' safety, while ensuring delivery of care. This policy applies to all personal (including, but not limited to, health) information ("information") owned by or entrusted to Mackenzie Health (MH).

## DEFINITION(S):

**Consent**[1] means "*the voluntary agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organization seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.*"

**Governance** refers to all of mechanisms, processes, and oversight bodies necessary to control and direct the program, including, but not limited to, its direction, implementation and governance documentation.

**Governance documentation** is the set of documents documenting MH's governance when related to the Privacy program. It includes, but is not limited to, the policies and procedures necessary to the efficiency of the program.

[1] Definition from the CSA standard *Q830-14 Model Code for the Protection of Personal Information*

**Individual** means any individual entrusting MH with their information like, but not limited to, patients, families, personnel etc…

**Information** is any personal information or personal health information owned, used by or entrusted to MH.

**Personnel** means any person that, with MH's authorization, acts for or on behalf of MH, like, but not limited to, employees (including temporary employees), physicians, nurse practitioners, mid-wives, allied healthcare professionals, students, volunteers, contractors and third party service providers providing services to MH.

**Personal Information** has the same meaning as defined in section 2 of the *Freedom of Information and Protection of Privacy Act* (FIPPA[2], and generally means non-health related identifying information about an individual in oral or recorded form. Examples include address, bank information, employment history, social insurance number, and any information that, directly or indirectly, identifies an individual. Note that, when associated with personal health information, personal information is deemed to be considered health related.

**Personal Health Information** has the same meaning as defined in section 4 of the *Personal Health Information Protection Act* (PHIPA)[3], and generally means identifying information about an individual in oral or recorded form, pertaining to that person's health or health services provided to the individual. Examples include family health history, health card number, and any information that, directly or indirectly, identifies an individual and links them to a healthcare provider.

**Privacy Specialists** means MH personnel supervised by the Privacy Office who possess the required Privacy professional designations, training and/or experience.

## PROCEDURE:

The Privacy program will use the 10 Privacy Principles established by the Canadian Standards Association's Model Code for the Protection of Personal Information as its foundation.

## 1 Privacy Principles

### 1.1 Accountability

The Board of Directors of MH is accountable to individuals for the protection and privacy of the information with which MH has been entrusted. MH is committed to ensuring the highest standard of privacy care and data protection is applied in the services it provides and technologies it manages.

[2] Available at https://www.ontario.ca/laws/statute/90f31#BK2
[3] Available at https://www.ontario.ca/laws/statute/04p03#BK5

The Board of Directors delegates authority to the Chief Executive Officer (CEO) to implement privacy and data protection measures at MH. The CEO designates the Chief Administrative Officer to act as the Chief Privacy Officer (CPO).

The CPO is responsible for overseeing MH's Privacy program. The CPO delegates the responsibility of implementing and managing this program throughout the organization to the Manager, Privacy & Information Security, who reports to the Chief Information Officer.

Key components of MH's privacy program include, but are not limited to:

- the necessary governance to support the effective management and operationalization of privacy in accordance with MH's legal, corporate and contractual requirements;
- a risk management practice to ensure privacy risks are managed at an acceptable level not only to MH but also to the individuals who entrusted their information to MH; and
- a network of individuals across the organization with specific privacy responsibilities.

Management at all levels of MH has primary responsibility for ensuring that information is identified and collected, used and/or disclosed within their department/unit or assigned area of management accountability. They are also responsible for taking the appropriate measures to prevent unauthorized access to or use, damage, loss, theft, or disclosure of information.

Employees also must take reasonable privacy precautions to prevent unauthorized collection, use, loss, theft, destruction, damage, misuse or disclosure of PHI in their care or custody.

Personnel shall comply with the requirements of this Policy, and any supporting governance documentation to appropriately protect the personal information in their care or custody, or which they use.

## 1.2 Identifying Purposes

MH shall document the purpose(s) for which personal information is collected, used and/or disclosed. Information must not be used and/or disclosed for purposes other than those for which it was collected, except with the appropriate consent of the individual or as permitted or authorized by law.

## 1.3 Consent

MH shall make a reasonable effort to ensure that the individual is advised of the purposes for which their information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

MH shall obtain consent voluntarily, at or before the time that personal information is collected, and not through coercion or deception. The type of consent sought out must be reasonable under the circumstances.

MH shall make reasonable effort to inform individuals about their privacy rights and the fact that they can withdraw their consent at any time.

### 1.4 Limiting Collection

MH shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfil the purposes identified. MH shall specify the type of information collected as part of their information-handling governance and practices.

### 1.5 Limiting Use, Disclosure, and Retention

MH shall only use the collected information for the purpose(s) identifies and provided to the individuals as per section 1.2 Identifying Purposes.

MH shall not retain the collected information longer than necessary to fulfil the identified purpose(s) and/or legally required.

### 1.6 Accuracy

MH shall strive to ensure the personal information it owns or it is entrusted with is kept as accurate as reasonably possible.

The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used.

### 1.7 Safeguards

Security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification and thus regardless of the format in which this information is held.

MH shall have an Information Security program to support the Privacy program's security requirements. The level of security applied should be reasonable under the circumstances.

### 1.8 Openness

MH shall be open about its governance and practices with respect to the management of personal information. Individuals shall be able to acquire information about MH's governance and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

The Privacy Office should be the primary point of contact should an individual require such information.

### 1.9 Individual Access

MH shall provide access to individuals to their own information within the legal timeframe (if any). This access includes, but is not limited to, how the information was used and to whom it was disclosed to.

As it is recognized that some information can be sensitive, MH shall make sure that the risk level of releasing such information is reasonable under the circumstances.

### 1.10 Challenging Compliance

The Privacy Office shall put procedures in place to receive and respond to complaints or inquiries about their governance and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.

All complaints shall be investigated. If a complaint is found to be justified, management shall take appropriate measures, including, if necessary, amending its governance and/or practices.

Individuals have the right to complain to the Information and Privacy Commissioner of Ontario if they believe that MH violated their privacy rights.

## 2 Responsibilities

The **Chief Administrative Officer** is responsible for:

- reporting to the board as required or to designate a substitute;
- ensure that Privacy goals are identified, that they meet organizational and legal requirements, and that they are addressed within the Privacy program.

**Corporate Procurement and anybody developing and/or managing contracts** are responsible for ensuring that all contracts require service providers to comply with this Policy and its supporting governance documentation or have their own governance documentation that is consistent with the requirements of this Policy.

**Health Information Services** is responsible for:

1. Acting as the official custodian of the legal medical record;
2. Addressing the good faith operations related to records management, retention/destruction, and the search and retrieval process/parameters of the legal medical record
3. Overseeing the appropriate access, release and disclosure of personal health information; and
4. Ensuring that the release of personal health information does not pose an unreasonable risk to the individual and/or to a 3rd party.

**Human Resources** are responsible for:

1. ensuring that this Policy and other awareness information are included in new-hire orientations; and
2. developing and administering processes for disciplining personnel for non-compliance with the Privacy program, in accordance with the laws of the jurisdiction.

**Management**, within their assigned area of responsibility, is responsible for:

1. ensuring all personnel are educated in this Policy and the governance documentation that support it,
2. ensuring this Policy is implemented effectively,
3. developing all necessary area specific governance documentation to support this Policy, and
4. identifying and protecting personal information. They are responsible for implementing all necessary privacy measures consistent with sound business practice, in compliance with corporate governance and regulatory requirements, and in line with any associated governance documentation.

The **Manager, Privacy & Information Security** is responsible and accountable for:

1. leading MH's Privacy program, which includes defining goals, objectives and metrics consistent with the corporate Strategic Plan to ensure that the organization's privacy principles, governance, and practices support the protection of the individuals' information;
2. managing and coordinating the design, implementation, operation and maintenance of MH's privacy governance within the defined scope; and
3. actively fostering a privacy culture by leading and supporting activities both internally and externally to increase awareness of MH's privacy principles, policies and procedures.

**Personnel** are responsible for:

1. complying with this Policy and the governance documentation that support it.
2. reporting (including self-reporting) instances of non-compliance, and participate in any corrective action, and
3. protecting the privacy of MH's patients and personnel.

The **Privacy Office** is responsible for:

1. managing the Privacy program, develop and maintain the necessary governance (including the necessary oversight body(ies) and documentation) to support this Policy, and provide feedback to senior management on the effectiveness of the program;
2. providing privacy specialists to meet the expectations set forth in this policy and deliver the privacy services part of the Privacy program;
3. providing a comprehensive and role-based privacy awareness and training program to comply with this Policy and its supporting governance documentation;
4. monitoring the effectiveness of the Privacy program;
5. auditing, and/or reviewing departments/units security practices and compliance with the Privacy program as required; and
6. serving as the point of contact to individuals.

**Senior Management** is responsible for providing the necessary guidance and support for the development and maintenance of the Privacy program, in line with privacy and legal requirements and business strategy objectives. This support includes, but is not limited to, the following:

1. Integrating privacy goals into relevant processes;
2. Providing clear direction and visible management support for privacy initiatives;
3. Providing the resources required for privacy; and
4. Approving assignment of specific roles and responsibilities for information security across the organization.

## REFERENCES:

- *Freedom of Information and Protection of Privacy Act*[4]
- *Personal Health Information Protection Act*[5]
- Canadian Standard Association standard *Q830-14 Model Code for the Protection of Personal Information*

[4] Available at https://www.ontario.ca/laws/statute/90f31
[5] Available at https://www.ontario.ca/laws/statute/04p03