Title: Management of Personal Health Information and Personal Information	**Policy No.:** AIMG 4.1.1 **Pages:** 12
Originator(s): Information and Privacy Office	**Initial Issue Date:** October 20, 2004
Owner: Information and Privacy Office	**Next Review Date:** May 28, 2022
Key Words: Privacy, Personal Health Information, Personal Information, IT Security, PHIPA, FIPPA, Privacy law, Privacy legislation, Privacy Breach, Patient rights	**Effective Date:** May 28, 2019
Reviewed by: Policy Subcommittee (PSC)	**Approved by:** Operations Committee (OPS)

1.0 Purpose

CAMH is committed to protecting the privacy and confidentiality of "personal health information" (PHI) and "personal information" (PI) in its custody or control.

As a health information custodian (HIC) as defined in the *Personal Health Information Protection Act* (PHIPA), and an institution as defined in the *Freedom of Information and Protection of Privacy Act* (FIPPA), CAMH is responsible for ensuring that the personal health information/personal information of its clients/patients and staff is managed in accordance with PHIPA, FIPPA, this policy, and other privacy related CAMH policies, procedures and protocols.

While this policy focuses on the personal health information/personal information of clients/patients and staff, where appropriate, it should be interpreted broadly to apply to any personal health information/personal information that CAMH holds except in the following circumstances:

- This policy does not deal with information regarding health care services administered under the direction of the CAMH Health and Wellness program, which is managed and protected in accordance with AHR 3.13.5 Confidentiality of Staff Health Information.
- This policy does not deal with personal health information contained in the records of the Client Relations Office, which is not collected or used for the purpose of providing health care. Such information is handled in accordance with PC 1.6.1 Client Relations.

2.0 Persons Affected

This policy applies to all agents of CAMH. Agents at CAMH include, but are not limited to, employees, physicians, courtesy appointees, volunteers, students, residents, fellows, consultants, vendors, and contractors.

3.0 Policy

CAMH has designated the Chief Privacy Officer (CPO) as the individual accountable for the overall management of personal health information/personal information in the custody or control of CAMH.

This policy is based on the following overarching principles:

- Individuals have a right to privacy and have a right to control how their personal health information/personal information is collected, used, disclosed, retained and disposed of subject to some exceptions.
- CAMH has a legal obligation to keep personal health information/personal information confidential. Such information cannot be disclosed without the individual's consent (i.e., permission) except as permitted or required by law.
- CAMH is authorized and directed by law to collect, use and disclose personal health information for the provision of health care, delivery of services, and certain administrative and other purposes. In some cases, CAMH and its agents are required by law to disclose personal health information.
- CAMH may collect, use and disclose personal health information in providing health care or health care services only to the minimum extent necessary to fulfill an identified purpose or for an otherwise authorized purpose. These "overarching principles" are discussed in more detail in sections 6.4 and 6.5.

It is expected that any Agent who comes into contact with personal health information/personal information of a client/patient or staff as part of their work at CAMH (clinical or non-clinical) shall abide by this policy, PHIPA and FIPPA.

4.0 Definitions

Agent: Includes any person who is authorized by CAMH to collect, use or disclose personal health information/ personal information on CAMH's behalf and for the purposes of performing services or activities for or on behalf of CAMH (*PHIPA*, 2004)

Client/patient: Anyone receiving care at CAMH or the individual's substitute decision maker (SDM) or, if deceased, the individual's estate representative.

Additionally, this may refer to a staff member who is also receiving care at CAMH as a client/patient.

***Freedom of Information and Protection of Privacy Act*, 1990 (FIPPA)**: Ontario's privacy legislation that governs the manner in which personal information may be collected, used, disclosed, retained and disposed.

Health information custodian (HIC): Refers to persons or custodians described in PHIPA who have custody or control of PHI as a result of the work they do. For example, doctors, nurses, social workers, pharmacists, physiotherapists, and psychologists as well as hospitals and psychiatric facilities are health information custodians (HICs).

Identifying information: includes information that could identify an individual for which it is reasonably foreseeable in the circumstances that it could be used either alone or with other information to identify an individual.

Institution: Refers to provincial ministries and most provincial agencies, boards and commissions, as well as colleges of applied arts and technology, universities and hospitals (as of January 1, 2012) to which FIPPA applies.

Personal health information (PHI): Identifying information about an individual, in oral or recorded form, if the information:

- Relates to the physical or mental health of the individual, including the individual's medical history and the individual's family medical history;
- 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 the payment or eligibility for health care;
- 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 care number; or
- Identifies an individual's substitute decision-maker.

Personal information (PI): Identifying information about an individual, in oral or recorded form, if the information:

- Relates to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or martial or family status of the individual;
- Relates 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 the 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 Health Information Protection Act, 2004 (PHIPA): Ontario's privacy legislation that governs the manner in which personal health information may be collected, used and disclosed within the health care system. It also regulates individuals and organizations that receive personal health information from health care professionals.

Privacy breach: includes any inadvertent or intentional theft or loss of personal health information/personal information; unauthorized collection, use or disclosure of personal health information/personal information; unauthorized modification or destruction of personal health information/personal information; or any non-compliance with this policy or other privacy-related policies, procedures and protocols.

Suspected Privacy Breach: Any occurrence or deviation that is detected and remediated before an incident occurs. Includes any event that has a potential to cause inadvertent or intentional theft or loss of personal health information/ personal information; unauthorized collection, use or disclosure of personal health information/personal information; unauthorized modification or destruction of personal health information/personal information; or any non-compliance with this policy or other privacy-related policies, procedures and protocols.

5.0 Responsibilities

5.1 All Staff

- Comply with this policy and related procedures and practices for the collection, use and disclosure of personal health information/personal information.
- Review and sign CAMH's Agreement to Comply with Policies and Procedures form.
- Ensure they have completed CAMH's privacy training and education.

- Ensure that an individual's privacy is upheld in accordance with this policy and ensure the confidentiality, integrity and availability of personal health information/personal information.
- Report all actual or suspected privacy breaches to the CAMH Information and Privacy Office (IPO).
- Where required, assist with requests for access to personal health information/personal information made by clients/patients or other individuals, SDMs, and estate representatives.
- Obtain clarity around privacy obligations where necessary.

5.2 Manager/Supervisor/Chief

- Ensure awareness, enforcement and compliance of relevant privacy policies, laws, procedures, protocols and practices.
- Ensure staff are up to date and have completed appropriate privacy training and education.
- Report all actual or suspected privacy breaches to the IPO.
- At the request of, and in coordination with the IPO, conduct and support investigations into suspected privacy breaches.
- Assist the IPO in responding to privacy queries and complaints.
- Receive and implement recommendations from the IPO regarding necessary actions following a breach, including the development of a breach notification and actions to prevent a reoccurrence.
- Receive and implement recommendations from the IPO regarding necessary actions following a privacy impact assessment.
- In consultation with Human Resources or the office of the Physician-in-Chief, take appropriate disciplinary action to ensure the incident is not repeated.
- Where requested, assist with client/patient or an individual's requests for access and correction and withdrawal of consent to their personal health information/personal information.

5.3 Information and Privacy Office

- Receive and respond to inquiries from staff and the public regarding CAMH privacy protocols, processes and practices, including PHIPA and FIPPA requirements.
- Contribute to the development of privacy policies, protocols, processes and practices specific to particular programs/projects.

- Assist in the development and provision of privacy education and training for CAMH agents regarding their responsibilities under privacy laws and CAMH privacy policies, protocols and procedures.
- Receive and respond to privacy complaints on behalf of CAMH.
- Ensure information is made publicly available regarding CAMH's privacy policies and practices.
- Investigate privacy incidents and/or suspected and actual privacy breaches.
- Provide assessments on the severity of a privacy breach to managers and Human Resources.
- Provide privacy risk/impact assessments on new collections, uses and/or disclosures.
- When necessary, consult with the Legal Office regarding legal interpretations, obligations and investigations of privacy breaches.
- When required, assist with requests for access or corrections to personal health information/personal information made by clients/patients, SDMs or estate representatives or other individuals.
- When required, assist with the implementation of a patient/client's consent directive.
- Monitor compliance with this policy and PHIPA/FIPPA by whatever means are appropriate to the circumstances.

5.4 Chief Privacy Officer

- Overall accountability for ensuring CAMH's compliance with this privacy policy and PHIPA/FIPPA.
- Responsible for annual reports to the CAMH Board of Trustees through the Audit and Finance Committee of the Board.
- Accountable for annual reports made to Ontario's Information and Privacy Commissioner with regard to PHIPA/FIPPA compliance and reporting of privacy breaches.
- Responsible for, where appropriate, reporting of breaches of PHIPA to regulatory colleges and/or to the Information and Privacy Commissioner of Ontario (IPC) for PHIPA/FIPPA breaches
- Accountable for the privacy and security of personal health information/personal information held in the custody or control of CAMH.
- Support the investigation of actual or suspected breaches of privacy or security and ensure breach notification is provided to affected individuals, including clients/patients and appropriate action is taken to prevent a reoccurrence, in accordance with PHIPA/FIPPA.

- Accountability for Personal Health Information:
    - The CPO is accountable for the management of personal health information/personal information collected, used, disclosed, retained, and disposed of by CAMH.
    - The CPO is accountable for the privacy and security of the personal health information/personal information collected, used, disclosed, retained and disposed of at CAMH.

5.5 Human Resources

- Ensure staff have reviewed and signed CAMH's Agreement to Comply with Policies and Procedures and maintain a copy of the form.
- Work with managers to determine appropriate disciplinary measures to be taken. Liaise with Legal Services to ensure organizational consistency in the application of privacy principles and contributing factors when determining appropriate disciplinary measures.
- Assist in the communication of required actions to other managers and staff where recommendations are to be implemented.
- Provide information necessary for IPO to fulfill its obligations under PHIPA/FIPPA.

5.6 Physician-in-Chief

- Ensure physicians have reviewed and signed CAMH's Agreement to Comply with Policies and Procedures and that the acknowledgement of awareness and understanding of PHIPA is signed as a part of the re-appointment process.
- Work with the relevant Physician Leadership to determine appropriate disciplinary measures to be taken. Discipline may involve the matter being put before the Medical Advisory Committee.
- Liaise with Legal Services to ensure organizational consistency in the application of privacy principles and contributing factors when determining appropriate disciplinary measures.
- Assist in the communication of required actions to other Physician Leaders where recommendations are to be implemented.
- Provide information necessary for IPO to fulfill its obligations under PHIPA.

6.0 Procedures

6.1 CAMH, as a health information custodian under PHIPA/institution under FIPPA, is responsible for protecting the privacy and security of personal health information/personal information in its custody and control and, as such, it shall:

- Implement policies and procedures to ensure the protection of personal health information/personal information.
- Educate staff regarding their responsibilities under CAMH's privacy policies and PHIPA/FIPPA when collecting, using, disclosing, retaining and disposing client/patient personal health information/individual's personal information.
- Implement policies and procedures outlining the responsibilities of the IPO to:
  - Receive and respond to complaints
  - Receive and respond to inquiries and requests on privacy-related matters
  - Make material on CAMH's privacy policies and procedures publicly available
  - Review the privacy policy, practices and processes on a regular basis
  - Investigate suspected privacy breaches to ensure remedial action is taken and reoccurrences are prevented.

6.2 Staff are expected to consult with the IPO and/or Legal Office regarding practices, training and expectations around the security and management of client/patient personal health information/individual's personal information.

6.3 Identifying Purposes for Which Personal Health Information/Personal Information is Being Collected

6.3.1 Staff will ensure that the individual from whom it collects personal health information is aware of the purposes for the collection.

6.3.2 Staff will consult with the IPO to ascertain whether the collection is lawful or if consent is required before the information can be collected for that purpose, if staff are uncertain.

6.4 Consent for the Collection, Use, and Disclosure of Personal Health Information

6.4.1 Staff will rely on implied consent from clients/patients or their legally authorized representative for the collection, use and disclosure of personal health information if the purpose is for the provision of health care and the other legal requirements are met.

6.4.2 Staff will obtain express consent to collect, use and disclose PHI when required. The manner in which CAMH seeks consent may vary depending on the circumstances and the type of information being collected, used or disclosed.

6.4.3 Staff will ensure that clients/patients are aware that consent may be withdrawn at any time, but the withdrawal cannot be retroactive for information already disclosed.

6.4.4 Staff can collect, use and disclose PHI without consent where PHIPA specifically requires or authorizes it (e.g., duty to report, serious risk of significant harm to self or others).

6.4.5 Staff may use personal health information for purposes unrelated to the provision of care if allowable by law. These circumstances may include purposes related to:

- administration and management of CAMH programs and services
- patient billing
- administration and management of the health care system
- research
- teaching
- statistical reporting
- fundraising
- as permitted or required by law.

6.5 Limiting Collection of Personal Health Information

6.5.1 CAMH will not collect personal health information/personal information indiscriminately. Both the amount and type of information collected will be limited to only what is necessary to fulfill the identified purpose.

6.5.2 Information is collected directly from the individual unless the law permits or requires collection from third parties (e.g., friends and family).

6.5.3 CAMH is authorized to collect personal health information from third parties without consent in order to examine, assess, observe or detain someone under the *Mental Health Act* and subject to relevant provisions of the *Criminal Code*.

6.6 Limiting Use, Disclosure, and Retention of Personal Health Information

6.6.1 Staff will limit the use, disclosure and retention of personal health information/personal information in accordance with this policy.

6.6.2 Staff will collect, use and disclose only the amount of personal health information/personal information required to meet the specified purpose or as otherwise authorized.

6.6.3 Requests for disclosure of personal health information must be made in accordance with AIMG 4.2.24 Disclosure of Personal Health Information from the CAMH Health Record.

6.6.4 Disclosures from the CAMH Health Record can be directed to the Health Records Department for consideration and processing.

6.6.5 Clarity regarding the authority to disclose personal health information can be obtained from the Health Records Department or the IPO.

6.6.6 Disclosures to law enforcement must be made under the direction of Risk Management or Legal Services.

6.6.7 Personal health information/personal information will be retained in accordance with AIMG 4.1.6 Retention and Storage of Records and as required by law.

6.7 Accuracy of Personal Health Information

6.7.1 To the extent possible, staff will ensure that client/patient personal health information/individual's personal information is as accurate, complete, and up to date as is necessary for the purposes for which it is to be used.

6.7.2 Individuals have a right to request corrections to their health records/personal information, subject to specific criteria as set out in PHIPA/FIPPA.

6.7.3 Requests for correction to records of PHI/PI in the custody or control of CAMH must be directed to the IPO upon receipt. The IPO will review such requests and determine if a correction to the record will be made. The IPO will respond to the requestor on behalf of CAMH in accordance with PHIPA/FIPPA requirements.

6.8 Safeguards for Personal Health Information

6.8.1 Staff are expected to be knowledgeable of and abide by this policy and other related privacy and security policies and practices and to obtain clarification of such policies and practices where necessary.

6.8.2 All staff are expected to be aware of the confidentiality of client/patient personal health information as outlined in the mandatory *Agreement to Comply with Policies and Procedures*.

6.8.3 Staff are expected to take all appropriate privacy training and education.

6.9 Openness of CAMH Personal Health Information/Personal Information Policies and Practices

Information about CAMH's policies and practices regarding the management of client/patient personal health information/individual's personal information is available to the public on CAMH's external website and through the IPO.

6.10 Challenging Compliance with CAMH's Privacy Policies and Practices

6.10.1 An individual may raise a concern or complaint regarding compliance with the privacy law, this policy or CAMH privacy practices to the IPO or CPO.

6.10.2 The IPO will receive and respond to complaints or inquiries about CAMH privacy policies and practices relating to the handling of client/patient personal health information/individual's personal information.

6.10.3 The IPO will investigate all privacy complaints. If a complaint is found to be justified, the IPO will make recommendations regarding appropriate corrective measures to be taken.

7.0 References

Personal Health Information Protection Act, 2004, S.O. 2004, c.3 Schedule Available at: http://www.elaws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm

Mental Health Act, 1990, R.S.O. 1990, c.M.7. Available at: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90m07_e.htm

Freedom of Information and Protection of Privacy Act, 1990, R.S.O., 1990, Chapter F.31. Available at: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_90f31_e.htm

Office of the Information and Privacy Commissioner, "Detecting and Deterring Unauthorized Access to Personal Health Information".

Office of the Information and Privacy Commissioner, "What to do when Faced with a Privacy Breach: Guidelines for the Health Sector".

8.0 Links/Related Documents

Agreement to Comply with Policies and Procedures
AHR 3.13.5 Confidentiality of Staff Health Information
AIMG 4.1.5 Storage of Personal Health Information on Mobile Computing Devices
AIMG 4.1.6 Privacy Incident Management Protocol

AIMG 4.2.24 Disclosure of Personal Health Information from the CAMH Health Record
PC 1.6.1 Client Relations

9.0 Review/Revision History

Date	Revision No.	Revision Type	Reference Section(s)
October 2004	1.0	New policy	n/a
June 2011	2.0	Complete	Procedures replaced by general principles
May 2015	3.0	Moderate	Reformat
April 2016	4.0	Moderate	Addition of references to Personal Information and FIPPA where relevant to ensure policy covers both personal and/or personal health information
May 2019	5.0	Minor	• Updated definitions for Agent, PHIPA, and Suspected Privacy Breach. • Minor updates to CPO responsibilities (moved from procedures section).