Title: Management of Personal Health Information and Personal Information	**Policy No.:** AIMG 4.1.1 **Pages:** 14
Originator(s): Information and Privacy Office	**Initial Issue Date:** October 20, 2004
Owner: Information and Privacy Office	**Next Review Date:** May 8, 2028
Key Words: Privacy, Personal Health Information, Personal Information, IT Security, PHIPA, FIPPA, Privacy law, Privacy legislation, Privacy Breach, Patient rights	**Effective Date:** May 9, 2025
Reviewed By: Director, Information and Privacy Office	**Approved By:** Policy Committee (PC)

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 CAMH personnel 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 CAMH personnel, 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's Health, Safety, and Wellness department, which is managed and protected in accordance with policy AHR 3.13.5 Confidentiality of CAMH personnel Health Information.
- This policy does not deal with personal health information contained in the records of the Patient and Family Experience Office (PFEO), which is not collected or used for the purpose of providing health care. Such information is handled in accordance with policy PC 1.6.1 Responding to Feedback (Complaints and Compliments) from Clients/Patients and Family.

2.0 Persons Affected

This policy applies to all CAMH personnel, including those who act as Agents of CAMH for the purpose of *PHIPA*. Agents at CAMH for the purpose of *PHIPA* include, but are not limited to, employees, physicians, courtesy appointees, volunteers, students, residents, fellows, consultants, vendors, and contractors.

3.0 Policy

3.1 CAMH has designated the Vice President, Digital health and Chief Information Officer as the individual accountable for the overall management of personal health information/personal information in the custody or control of CAMH.

3.2 This policy is based on the following overarching principles:

- individuals have a right to consent to the collection, use and disclosure of their personal health information/personal information subject to some exceptions;
- CAMH has a legal obligation to keep personal health information/personal information confidential;
- CAMH is legally authorized in some circumstances to collect, use and disclose personal health information without consent for the provision of health care and other activities as permitted or required by law;
- CAMH may collect, use and disclose personal health information in providing health care or health care services only where identifying information is required and 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, below.

3.3 CAMH Agents who have access to personal health information/personal information of a client/patient or CAMH personnel as part of their work at CAMH (clinical or non-clinical) shall abide by this policy and all applicable privacy legislation.

4.0 Definitions

Agent: Any personnel who is authorized by CAMH to collect, use or disclose personal health information on CAMH's behalf and for the purposes of performing services or activities for or on behalf of CAMH (PHIPA).

***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): Any persons or organizations who have custody or control of personal health information as a result of the work they do, including operators of hospitals and designated psychiatric facilities.

Identifying information: Information that identifies an individual or 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;
- is a plan that sets out the home and community care services for the individual to be provided by a health service provider or Ontario Health Team pursuant to funding under section 21 of the *Connecting Care Act, 2019*;
- relates to payments or eligibility for health care, or eligibility for coverage 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 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 health information custodians as well as individuals and organizations that receive personal health information from health information custodians.

Personal information (PI): Identifying information about an individual, in 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.

Privacy Breach: Any inadvertent or intentional theft or loss (including electronic personal health information being made unavailable for use due to unauthorized encryption) of personal health information/personal information; unauthorized use or disclosure of personal health information/personal information (including electronic personal health information that is encrypted due to ransomware, even if there is no evidence of access or transfer); unauthorized collection, use or disclosure of personal health information through the electronic health record (i.e., ConnectingOntario); unauthorized modification or destruction of personal health information/personal information.

Suspected Privacy Breach: Any occurrence or deviation that is detected and premediated before the Information and Privacy Office has confirmed if it is a privacy breach. Includes any event that has a potential to cause inadvertent or intentional theft or loss (including electronic personal health information being made unavailable for use due to unauthorized encryption) of personal health information/ personal information; unauthorized use or disclosure of personal health information/personal information (including electronic personal health information that is encrypted due to ransomware, even if there is no evidence of access or

transfer); unauthorized collection, use or disclosure of personal health information through the electronic health record (i.e., ConnectingOntario); unauthorized modification or destruction of personal health information/personal information.

5.0 Responsibilities

5.1 All CAMH Personnel

- 5.1.1 Comply with this policy and related procedures and practices for the collection, use and disclosure of personal health information/personal information.
- 5.1.2 Review and sign CAMH's Agreement to Comply with Policies and Procedures Form.
- 5.1.3 Complete CAMH's required privacy training and education.
- 5.1.4 Report all actual or suspected privacy breaches to the Information and Privacy Office (IPO).
- 5.1.5 Where required, assist with requests for access to personal health information/personal information made by clients/patients or other individuals, substitute decision-makers (SDMs), and estate representatives.
- 5.1.6 Consult IPO to obtain clarity regarding privacy obligations where necessary.

5.2 Manager/Supervisor/Chief

- 5.2.1 Ensure awareness, enforcement and compliance of relevant privacy policies, laws, procedures, protocols and practices by CAMH personnel.
- 5.2.2 Ensure CAMH personnel are up to date and have completed required privacy training and education.
- 5.2.3 Report all actual or suspected privacy breaches to the IPO.
- 5.2.4 At the request of, and in coordination with the IPO, conduct and support investigations into suspected privacy breaches.
- 5.2.5 Assist the IPO in responding to privacy queries and complaints.
- 5.2.6 Receive and implement recommendations from the IPO regarding necessary actions following a breach, including the development of a breach notification plan and actions to prevent a reoccurrence.
- 5.2.7 Receive and implement recommendations from the IPO regarding necessary actions following a privacy impact assessment.
- 5.2.8 In consultation with People and Experience (P&E) or the office of the Chief Medical Officer, take appropriate disciplinary action in response to a privacy breach or non-compliance with expectations in this policy.

5.2.9 Where requested by IPO, assist IPO in responding to a client/patient or an individual's requests regarding their personal health information/ personal information, including requests for access, correction, consent directives, complaints or concerns.

5.3 Information and Privacy Office

5.3.1 Receive and respond to inquiries from CAMH personnel and the public regarding CAMH privacy protocols, processes and practices, including PHIPA and FIPPA requirements.

5.3.2 Contribute to the development of privacy policies, protocols, processes and practices specific to particular CAMH programs/projects.

5.3.3 Assist in the development and provision of privacy education and training for CAMH personnel regarding their responsibilities under privacy laws and CAMH privacy policies, protocols and procedures.

5.3.4 Receive and respond to privacy concerns or complaints on behalf of CAMH.

5.3.5 Ensure information is made publicly available regarding CAMH's privacy policies and practices.

5.3.6 Investigate privacy incidents and/or suspected and confirmed privacy breaches.

5.3.7 Provide assessments on the severity of a privacy breach to relevant CAMH personnel, including managers and P&E.

5.3.8 Conduct privacy risk/impact assessments on new collections, uses and/or disclosures of personal health information/personal information.

5.3.9 Provide consultation and advice in the review of legal agreements regarding privacy implications and the inclusion of relevant privacy provisions.

5.3.10 When necessary, consult with Legal Services regarding the interpretation of legal obligations and regarding the investigation and response to actual or suspected privacy breaches.

5.3.11 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.

5.3.12 When required, assist with the implementation of a patient/client's consent directive.

5.3.13 Monitor compliance with this policy and PHIPA/FIPPA by whatever means are appropriate to the circumstances.

5.4 Vice President, Digital Health and Chief Information Officer

5.4.1 Overall accountability for ensuring CAMH's compliance with this privacy policy and PHIPA/FIPPA.

5.4.2 Responsible for annual reports to the Board of Trustees through the Audit and Finance Committee of the Board.

5.4.3 Accountable for annual reports made to Ontario's Information and Privacy Commissioner with regard to PHIPA/FIPPA compliance and reporting of privacy breaches.

5.4.4 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.

5.4.5 Accountable for the privacy, security and management of personal health information/personal information held in the custody or control of CAMH.

5.4.6 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.

5.5 People and Experience

5.5.1 Ensure CAMH personnel have reviewed and signed the Agreement to Comply with Policies and Procedures Form and maintain a copy.

5.5.2 Consult with managers and Legal Services in determining the appropriate disciplinary measures to be taken in the event of non-compliance with this policy or relevant privacy legislation

5.5.3 Assist in the communication of required actions to other managers and CAMH personnel where recommendations are to be implemented.

5.5.4 Provide information necessary for IPO to fulfill its obligations under PHIPA/FIPPA.

5.6 Chief Medical Officer

5.6.1 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.

5.6.2 Consult with relevant physician leadership and Legal Services to determine appropriate disciplinary measures to be taken in the event of non-compliance with this policy or relevant privacy legislation.

Discipline may involve the matter being put before the Medical Advisory Committee.

5.6.3 Assist in the communication of required actions to other Physician Leaders where recommendations are to be implemented.

5.6.4 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:

6.1.1 implement policies and procedures to ensure the protection of personal health information/personal information;

6.1.2 educate CAMH personnel 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;

6.1.3 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; and
- investigate actual and suspected privacy breaches to ensure remedial action is taken and reoccurrences are prevented.

6.2 As agents of CAMH, CAMH personnel will:

6.2.1 consult with the IPO, IT Security and/or Legal Services regarding practices, training and expectations around the security and management of client/patient personal health information/individual's personal information;

6.2.2 be aware of the confidentiality of client/patient personal health information as outlined in the mandatory Agreement to Comply with Policies and Procedures Form.

6.3 CAMH personnel are expected to take all appropriate privacy training and education upon hire and yearly thereafter.

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

6.4.1 CAMH personnel will ensure that the individual from whom it collects personal health information is aware of the purposes for the collection.

6.4.1.1 CAMH personnel will consult with the IPO to ascertain whether the collection is lawful, and/or if consent is required before the information can be collected for that purpose, if CAMH personnel are uncertain.

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

6.5.1 CAMH personnel may rely on implied consent from clients/patients or their legally authorized representative for the collection, use and disclosure of personal health information if

6.5.1.1 the information is collected, used or disclosed with another Health Information Custodian and/or the client/patient; and

6.5.1.2 the purpose is for the provision of health care.

6.5.2 CAMH personnel will obtain express consent to collect, use and disclose personal health information when required (e.g., disclosing personal health information to a client/patient's lawyer or insurance company).

6.5.3 The manner in which CAMH personnel obtains consent may vary depending on the circumstances and the type of information being collected, used or disclosed.

6.5.4 CAMH personnel will inform clients/patients that consent may be withdrawn at any time, but the withdrawal cannot be retroactive for information already used or disclosed.

6.5.5 CAMH personnel can collect, use and disclose personal health information without consent only where PHIPA specifically requires or authorizes it (e.g., mandatory reporting obligation, a situation of significant risk of serious harm to self or others).

6.5.6 CAMH personnel may use personal health information for purposes unrelated to the provision of care if authorized by law. These circumstances may include purposes related to:

- administration and management of CAMH programs and services;
- client/patient billing;
- administration and management of the health care system;
- research;
- teaching;
- statistical reporting;
- de-identify personal health information, including to provide non-identifiable data to third-parties for their own purposes;
- fundraising; and/or
- as permitted or required by law.

6.6 Limiting Collection of Personal Health Information

6.6.1 Both the amount and type of personal health/personal information collected by CAMH personnel will be limited to only what is necessary to fulfill the identified purpose and only when identifiable information is needed.

6.6.2 Personal health information/personal information will be collected directly from the individual to whom it relates, unless the law permits or requires collection from third parties (e.g., friends and family).

6.6.3 CAMH is authorized to collect personal health information from third parties without consent when obtaining consent is not possible, and such information is necessary to:

6.6.3.1 examine, assess, observe or detain someone under the *Mental Health Act*, or

6.6.3.2 when such information is necessary to comply with Part XX.1 of the *Criminal Code* or an order or disposition made pursuant to this Part.

6.6.3.3 CAMH personnel will consult with Legal Services for assistance in understanding the disclosure authority under this section, if required.

6.7 Limiting Use, Disclosure and Retention of Personal Health Information

6.7.1 CAMH personnel will limit the use, disclosure and retention of personal health information/personal information in accordance with this policy.

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

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

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

6.7.5 CAMH personnel will consult with the Health Records Department, the IPO and/or Legal Services for clarity regarding the authority to disclose personal health information.

6.7.6 Disclosure of personal health information/personal information to law enforcement agencies will be made in accordance with policy AHR 3.14.17 Communicating with Police

6.7.7 Personal health information/personal information will be retained in accordance with policies AIMG 4.2.5 Retention of Records of Clinical Care and AIMG 4.1.6 Retention and Storage of Records and as required by law.

6.8 Accuracy of Personal Health Information

6.8.1 CAMH personnel will take reasonable steps to 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.

6.8.2 Requests by an individual for correction to records of personal health information/personal information in the custody or control of CAMH will 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.

6.9 Safeguards for Personal Health Information

6.9.1 CAMH personnel are expected to be knowledgeable of and abide by this policy and other related privacy and security policies and practices to ensure that personal health information and personal information is protected against theft, loss and unauthorized use or disclosure as well as unauthorized copying, modification or disposal.

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

6.10.1 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.

6.11 Challenging Compliance with CAMH's Privacy Policies and Practices

6.11.1 Questions or complaints about privacy policies or practices at CAMH may be addressed to the Information and Privacy Office, (416) 535-8501 ext. 33314, or privacy@camh.ca.

6.11.2 The IPO will receive, investigate 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.

6.11.3 If a complaint is found to be justified, the IPO will make recommendations to relevant CAMH leadership regarding appropriate corrective measures to be taken.

7.0 References

Criminal Code R.S.C., 1985, c. C-46. Available at: https://laws-lois.justice.gc.ca/eng/acts/c-46/

Freedom of Information and Protection of Privacy Act, 1990, R.S.O., 1990, Chapter F.31. Available at: https://www.ontario.ca/laws/statute/90f31

Mental Health Act, 1990, R.S.O. 1990, c.M.7. Available at: https://www.ontario.ca/laws/statute/90m07

Office of the Information and Privacy Commissioner of Ontario.

Office of the Information and Privacy Commissioner of Ontario. Circle of Care. Available at: https://www.ipc.on.ca/sites/default/files/legacy/Resources/circle-of-care.pdf

Office of the Information and Privacy Commissioner of Ontario. Detecting and Deterring Unauthorized Access to Personal Health Information. Available at: https://www.ipc.on.ca/en/resources-and-decisions/detecting-and-deterring-unauthorized-access-personal-health-information

Office of the Information and Privacy Commissioner of Ontario. Responding to a Health Privacy Breach: Guidelines for the Health Sector. Available at: https://www.ipc.on.ca/en/resources-and-decisions/responding-health-privacy-breach-guidelines-health-sector

Personal Health Information Protection Act, 2004, S.O. 2004, Chapter 3, Schedule A. Available at: https://www.ontario.ca/laws/statute/04p03

8.0 Links/Related Documents

8.1 Related Policies, Procedures, Medical Directives, and Delegations

AHR 3.13.5 Confidentiality of CAMH Personnel Health Information
AHR 3.14.17 Communicating with Police
AIMG 4.1.5 Storage of Personal Health Information/Personal Information on Mobile Computing Devices
AIMG 4.1.6 Retention and Storage of Records
AIMG 4.1.6 Privacy Incident Management Protocol
AIMG 4.1.20 Storage of Personal Health Information, Sensitive and Confidential Information in the Cloud
AIMG 4.1.21 Service Provider
AIMG 4.2.5 Retention of Records of Clinical Care
AIMG 4.2.24 Disclosure of Personal Health Information from the CAMH Health Record
HSR 227 – Privacy Requirements in Research (Research Operations, Services and Supports-specific SOP)
PC 1.6.1 Responding to Feedback (Complaints and Compliments) from Clients/Patients and Family

8.2 Related Forms

Agreement to Comply with Policies and Procedures (Administrative Form)

8.3 Other Resources

N/A

9.0 Review/Revision History

Date	Revision No.	Revision Type (minor edit, moderate revision, complete revision)	Reference Section(s)
October 2004	1.0	New policy	• N/A.
June 2011	2.0	Complete revision	• Procedures replaced by general principles.
May 2015	3.0	Moderate revision	• Reformat.
April 2016	4.0	Moderate revision	• Addition of references to Personal Information and FIPPA where

Date	Revision No.	Revision Type (minor edit, moderate revision, complete revision)	Reference Section(s)
			relevant to ensure policy covers both personal and/or personal health information.
May 2019	5.0	Minor edit	• Updated definitions for Agent, PHIPA, and Suspected Privacy Breach. • Minor updates to CPO responsibilities (moved from procedures section).
May 2022	6.0	Minor edit	• Updated links (including correcting policy names). • Minor wordsmithing for consistency. • Reformat.
May 2023	6.1	Minor edit	• Updated links (changed from e-law to Ontario.ca URLs).
May 2025	7.0	Minor edit	• Masthead – updated Review and Approval Authorities. • Sections 3.0 and 6.4.6 – updated authorized use to include de-identification of PHI, including to give the resulting data to third-parties. • Section 4.0 – updated definitions to align with legislation. • Throughout – wordsmith, re-arranging content, and removing duplicate language.