Title: CAMH Service Provider Privacy	**Policy No.:** AIMG 4.1.10
	Pages: 9
Originator(s): Privacy/Legal	**Initial Issue Date:** April 2016
Owner: Privacy	**Next Review Date:** April 2019
Key Words:	**Effective Date:** May 1, 2016
Reviewed by: Privacy, Legal Services, DATIS Program	**Approved by:** Chief Privacy Officer

1.0 Purpose

This policy defines the privacy obligations and responsibilities of the Centre for Addiction and Mental Health in its capacity as a Service Provider (i.e., an electronic service provider or health information network provider, as these terms are defined in the *Personal Health Information Protection Act (PHIPA), 2004*. When acting in the role of Service Provider, CAMH is providing services to one or more health information custodians (HICs) that involve the use and retention by CAMH of Personal Health Information (PHI) in the custody of the HICs.

2.0 Persons Affected

This policy applies to all CAMH Personnel who carry out activities on behalf of CAMH in respect of its role as a Service Provider to one or more HICs.

3.0 Policy

3.1 CAMH will establish its authority to use PHI as a Service Provider to HICs through Agreements with each HIC to which CAMH provides services.

Agreements with HICs will:

- require CAMH to follow all PHIPA requirements placed on electronic service providers and health information network providers when CAMH is acting in these roles;
- indicate the purposes for which HICs collect, use and disclose the PHI that CAMH as a Service Provider uses and retains on behalf of the HICs;
- permit CAMH to use and retain PHI only in a manner that a HIC is permitted to use PHI.

3.2 CAMH will use PHI of HICs for the HICs' purposes as set out in Agreements with HICs, and never for its own purposes.

3.3 Each CAMH department acting on CAMH's behalf as a Service Provider will designate a CAMH employee as a Privacy Designate, who will, in consultation with the Information and Privacy Office (IPO), be responsible for ensuring the department meets the requirements of this policy.

The Privacy Designate, in consultation with the IPO, will conduct the following activities in fulfillment of her or his privacy responsibilities within her or his department:

- Deliver privacy and security training to CAMH Personnel that addresses CAMH's role as a Service Provider;
- Ensure appropriate Agreements are entered into with all third party service providers retained to assist the department in managing PHI in the custody of HICs, which include terms that bind the third party service provider to the same privacy obligations as CAMH's privacy obligations to HICs;
- Conduct monitoring activities to determine compliance of CAMH Personnel with CAMH's privacy obligations as a Service Provider;
- Create and post a notice that describes in plain language:
    - the services that the CAMH department provides to HICs
    - a description of the information security safeguards that the CAMH department has deployed to protect the PHI it has retained on behalf of HICs against unauthorized access, use, disclosure or alteration (including disposal)
    - how a member of the public can contact the Privacy Designate for the CAMH department to ask questions and receive information about the privacy safeguards deployed by CAMH within the department
    - Any legislative requirements to which the CAMH department, in its role as Service Provider, is subject.

3.4 Management of privacy incidents and breaches

3.4.1 In consultation with the IPO, a CAMH Privacy Designate will immediately notify a HIC when PHI of the HIC has been subject to unauthorized access, use, disclosure, or alteration (including disposal) due to activities of CAMH Personnel, or within the CAMH technical or business environment.

3.4.2 The Privacy Designate will follow AIMG 4.1.6 Privacy Incident Management Protocol to manage and contain privacy incidents and breaches affecting PHI of a HIC.

3.4.3 CAMH will securely communicate to HICs affected by a privacy incident or breach the full scope of information each HIC requires to conduct its own notifications to its clients/patients.

3.5 Consent

In its role as a Service Provider, CAMH will have no responsibility for, and will not participate in any processes for, obtaining lawful consent for the collection, use and disclosure of PHI by HICs. Obtaining lawful consent is solely the responsibility of each HIC.

3.6 Access to and Use of PHI

3.6.1 CAMH will use PHI of a HIC only to support the purposes and provide the specific services identified in its Agreement with the HIC.

3.6.2 CAMH will not use PHI of a HIC for its own purposes.

3.6.3 CAMH will maintain procedures for:

- granting CAMH Personnel with access to PHI of HICs, and documenting the scope and purpose of access for CAMH Personnel
- monitoring the access by CAMH Personnel to PHI of HICs
- revoking the access of CAMH Personnel to PHI of HICs, so that Personnel will not have access to PHI when departing from CAMH, or completing duties to the HICs

3.6.4 CAMH Personnel will limit their access to and use of PHI to ensure that they only use or access PHI required to provide services to HICs.

3.7 Disclosure of PHI

CAMH will not disclose PHI of a HIC to any individual or third party unless

- authorized to do so by the HIC that is the custodian of the PHI
- required to do so by law

3.8 Retention and disposal of records of PHI in the custody of HICs

3.8.1 Retention periods for all PHI of HICs will be defined in CAMH's Agreement with each HIC.

3.8.2 CAMH will retain PHI of HICs using only systems and methods defined in CAMH's Agreement with each HIC.

3.8.3 CAMH's Agreements with HICs will indicate whether the PHI retained by CAMH is the HIC's original version of the PHI, or a copy.

3.8.4 CAMH will not dispose of PHI of HICs unless explicitly authorized to do so in its Agreement with a HIC.

3.8.5 CAMH will follow its internal procedures for secure disposal of PHI of HICs, and will provide HICs with a certificate of destruction for any records of PHI.

3.9 Retention and disposal of copies of PHI made by CAMH

3.9.1 CAMH Personnel will not make copies of PHI of HICs in any form, except to provide the services defined in the Agreement with the HIC.

3.9.2 CAMH Personnel will immediately and securely dispose of copies of PHI they have made as soon as they have fulfilled the purposes for which the copies were made.

3.10 Accuracy

CAMH will not alter PHI it manages on behalf of HICs in any way unless the alteration:

- is described in CAMH's Agreement with the HIC as an authorized use of the PHI;
- has been requested in writing by the HIC, and the Privacy Designate, in consultation with the IPO, has reviewed the request and explicitly authorized CAMH Personnel to make the alteration.

3.11 Safeguards

3.11.1 CAMH will deploy information security safeguards (including physical, technical and administrative safeguards) to protect PHI of HICs from unauthorized collection, access, use, disclosure, alteration or disposal.

3.11.2 CAMH information security safeguards will be deployed in accordance with the ISO 27002 standard *Information technology — Security techniques — Code of practice for information security management*.

3.11.3 CAMH information security safeguards will include, but not be limited to:

- access controls for all systems, whether electronic or not electronic, in which CAMH retains records of PHI of HICs, and which require CAMH Personnel to provide valid and controlled credentials before being provided with access to the systems;
- data security measures that protect PHI in retention (e.g., encrypted storage) or when it is transmitted between a HIC and CAMH (e.g., encrypted connections);
- network security safeguards to protect CAMH electronic systems from intrusion or compromise by malicious software and other such threats;
- physical security safeguards for all environments housing systems used to retain PHI of HICs (e.g., locked server rooms).

3.12 Access and correction requests

CAMH will support HICs in responding to access and correction requests received by a HIC by:

- providing the HIC, on request, the records of the HIC, within 5 business days of receipt of the request from the HIC;
- forwarding to a HIC any requests from the HIC's clients/patients for access to or correction of a client/patient's records of PHI retained by CAMH in its role as a Service Provider to the HIC, and not responding to these requests directly.

3.13 Privacy inquiries

CAMH will respond to privacy inquiries regarding the services it provides to HICs to manage their PHI by:

- forwarding the inquiry to the relevant HICs, if the inquiry pertains specifically to the privacy practices of the HICs;
- responding directly to the inquiry if it pertains to CAMH's own privacy practices, and notifying the HICs to which CAMH provides the relevant services of the receipt and response to the inquiry.

3.14 Privacy complaints

3.14.1 CAMH will support HICs in responding to privacy complaints that are received by HICs that relate to the services provided to the HICs by CAMH.

3.14.2 CAMH will forward to HICs any privacy complaints it receives directly regarding the privacy practices of the HICs identified in the complaint.

3.14.3 CAMH will address privacy complaints about its services to HICs in accordance with its internal complaints management policy and procedure, and notify all HICs regarding the receipt of the complaint, and the outcome of the complaint management process.

3.14.4 CAMH will cooperate with a HIC if the HIC believes that CAMH's response to a complaint about its privacy practices did not adequately meet CAMH's privacy responsibilities as a Service Provider to the HIC.

3.15 Privacy audit

3.15.1 CAMH will conduct scheduled privacy audit activities to determine whether or not CAMH Personnel are in compliance with CAMH's privacy obligations as a Service Provider.

3.15.2 Privacy Designates will report the results of all privacy audit activities to the IPO.

3.15.3 CAMH will provide HICs with the results of its privacy audits on request.

3.15.4 CAMH will conduct privacy audit activities at the request of a HIC, to support a HIC in managing or investigating a privacy incident or privacy complaint.

4.0 Definitions

Agreement: A contract between CAMH and a third party (e.g., a HIC, a third party service provider) that defines services that each party will provide to the other, and the associated obligations, including privacy obligations, of each party for the delivery of the services. Where CAMH acts as a Service Provider to one or more HICs (by providing services as an electronic service provider or health information network provider), it will execute an Agreement with the HIC for the provision of the services.

CAMH Personnel: Any member(s) of the academic, non-academic or medical staff at CAMH, including but not limited to employees, individuals with a medical appointment, researchers, research support staff, undergraduate and graduate students, post-doctoral fellows, agents, contractors, and volunteers using CAMH facilities, equipment or resources.

Health Information Custodian (HIC): As defined in section 3 of the *Personal Health Information Protection Act (PHIPA), 2004*, a HIC) provides CAMH with access to PHI in its custody, and for which CAMH acts as a Service Provider (i.e., an electronic service provider or health information network provider as these terms are defined in PHIPA).

Information and Privacy Office (IPO): The CAMH Office which is overseen by the CAMH Chief Privacy Officer, and which has responsibility for ensuring CAMH's compliance with its PHIPA obligations.

Personal Health Information (PHI): Any identifying information about an individual's health status or health care, including information that:

- relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
- relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
- is a plan of service within the meaning of the *Home Care and Community Services Act, 1994* for the individual,
- 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 (PHIPA), 2004: The provincial legislation governing the collection, use and disclosure of PHI by HICs.

Privacy Designates: CAMH Personnel within CAMH departments that provide services to HICs requiring access to and use of PHI in the custody of the HICs, who have been designated as the individuals responsible for ensuring each department's compliance with CAMH's privacy obligations as a Service Provider. Where no such person has been designated within the department, the Privacy Designate will be an individual within the IPO (as appropriate).

Service Provider: The role that CAMH holds when it provides services to and/or on behalf of a HIC, and uses and/or retains PHI in the custody of the HIC for the HIC's purposes, and not for CAMH's own purposes.

5.0 Responsibilities

The **Privacy Designate** in each CAMH department that provides services to HICs is responsible for ensuring that the CAMH Personnel within the department have met the requirements of this policy.

The **CAMH IPO** is responsible for ensuring that each Privacy Designate has met her or his responsibilities under this policy.

6.0 Procedures

Making and managing copies of records of PHI

CAMH Personnel who print paper copies or make electronic copies of PHI in the custody of HICs must:

- Document the creation of copies of PHI in a *Log of Copies of PHI* that is maintained by the Privacy Designate, and include in the documentation:
    - the purpose for making the copy
    - the date and time when the copy was made
    - the scope of PHI that was copied
    - the date and time on which CAMH Personnel anticipate disposing of the copy
- Securely retain the copied PHI in the following manner when it is not in use:
    - paper copies of PHI should be retained in a locked cabinet, in a folder or envelope that indicates that the paper copy is PHI and should not be accessed
    - electronic copies should be retained on a drive within the CAMH network to which only named CAMH Personnel within the CAMH department have access after approval by the Privacy Designate

- Not remove the copied PHI from the CAMH environment under any circumstances.
- Securely dispose of the copied PHI immediately after the purpose for which the copy was made has been fulfilled, using the following methods:
    - paper copies will be shredded in a commercial cross-cut shredder
    - electronic records will be permanently deleted in accordance with the Service Provider Retention and Disposal Policy and Procedures
- Document the disposal of the copied PHI in the Log of Copies of PHI.

7.0 References

This CAMH Service Provider Privacy Policy is supported by the following CAMH privacy and security procedures:

- Procedures for Execution of Agreements with Third Party Service Providers
- Procedures for Limiting Access to PHI
- Service Provider Logging and Auditing Procedure
- Service Provider Privacy Incident Management Procedure
- Procedure for Managing Requests for De-Identified Research Data
- Procedures for Retention and Disposal of PHI

8.0 Links/Related Documents

n/a

9.0 Review/Revision History

Date	Revision No.	Revision Type (minor edit, moderate revision, complete revision)	Reference Section(s)
	1.0	New policy	n/a