Title: Service Provider Procedures for Limiting Access to Personal Health Information	**Procedure No.:** AIMG 4.1.15 **Pages:** 5
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 Procedure Description

This procedure defines how CAMH will appropriately limit access of CAMH Personnel to Personal Health Information (PHI) of Health Information Custodians (HICs) that is used and/or retained by CAMH in its role as a Service Provider.

2.0 Persons Affected

In consultation with the Information and Privacy Office (IPO), the procedures in this document will be conducted by the Privacy Designate in each CAMH department that acts as a Service Provider to one or more HICs.

3.0 Definitions

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 Protection Act (PHIPA), 2004: The provincial legislation governing the collection, use and disclosure of PHI by HICs.

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.

Privacy Designates: CAMH Personnel within CAMH departments that provide services to HICs requiring access to and use of PHI 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 of the HIC for the HIC's purposes, and not for CAMH's own purposes.

4.0 Procedures

4.1 Maintenance of Roles and Permissions List

The Privacy Designate will maintain a Roles and Permissions List for the department for which she or he is responsible.

The Roles and Permissions List will identify the roles of CAMH Personnel that have access to PHI and, for each role, the following information:

- user role title
- purposes for the role's access to PHI
- systems the role can access
- scope of PHI the role can access
- permitted uses of the PHI

The Privacy Designate will distribute permissions in the Roles and Permissions List to prevent a concentration of access to PHI in one specific role.

4.2 Documenting and approving access of CAMH Personnel to PHI

The Privacy Designate will

- Assess the need of CAMH Personnel in her or his department to access PHI, and assign one or more roles to CAMH Personnel from the Roles and Permissions List
- Use the *Access Assignments Form* to document the name, user role, PHI access permissions, employment start date for CAMH Personnel, and date the log will be reviewed
- Provide the IPO with a copy of each *Access Assignments Form* for CAMH Personnel and store the original document in a secure location
- Ensure that CAMH Personnel sign the Access Assignments Form to agree that access to PHI will be only as described on the Form
- Send a copy of the signed Form to CAMH Human Resources to place in the file of CAMH Personnel
- Ensure CAMH Personnel have been provisioned with access to systems that corresponds to the access described on the Form
- Provide CAMH Personnel with keys or other physical controls assigned to their access level and document these transactions on a *Personnel Asset Log* form.

4.3 Monitoring access of CAMH Personnel to PHI

On an annual basis, the Privacy Designate will:

- Review the *Access Assignments Forms* to determine if there have been any changes to the access of CAMH Personnel to PHI in the previous year
- Determine the reason for any changes to the access of CAMH Personnel to PHI, and either revoke the changed access or document it in the appropriate *Access Assignments Form*

4.4 Modifying access of CAMH Personnel to PHI

4.4.1 If the Privacy Designate determines that CAMH Personnel require a reduced scope of access to PHI, she or he will:

- Document the reasons for the change on the *Access Assignment Form*, and indicate if there are disciplinary reasons for the change
- Revise the relevant *Access Assignment Form* to reflect the change
- Modify the user account and permissions of relevant CAMH Personnel to reflect the new status

4.4.2 If the Privacy Designate determines that CAMH Personnel require an increased scope of access to PHI, she or he will:

- Document the reasons for the change and why the increased scope of access is required to provide services to the HICs
- Revise the relevant *Access Assignment Form* to reflect the change
- Modify the user account and permissions of relevant CAMH Personnel to reflect the new status

4.5 Revoking access of CAMH Personnel to PHI

When the Privacy Designate learns or determines that CAMH Personnel will leave CAMH, she or he will complete the following steps *before the departure of Personnel from CAMH*:

- Collect all physical and information assets provided to CAMH Personnel (corporate documents, software, electronic devices, keys and access badges, etc.)
- Record the returned assets on the *Personnel Asset Log* form
- Request in writing that CAMH Personnel return any outstanding assets

- Ensure that access of CAMH Personnel to all CAMH systems has been revoked, or will be revoked on the day of the departure of relevant CAMH Personnel
- Indicate in the relevant *Access Assignments Form* that the access of departing CAMH Personnel to all CAMH systems has been withdrawn

5.0 References

n/a

6.0 Links/Related Documents

n/a

7.0 Review/Revision History

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