Team Name: Health Information Services Team Lead: Privacy and Access Specialist Approved by:	Reference Number: ORG.1411.PL.203 Program Area: Health Information Services Policy Section: Privacy and Access
Issue Date: January 13, 2016 Review Date: Revision Date: July 13, 2022	Subject: Reporting and Investigating Privacy Breaches and Complaints

Use of pre-printed documents: Users are to refer to the electronic version of this document located on the Southern Health-Santé Sud Health Provider Site to ensure the most current document is consulted.

*Words beginning with a capital letter may be found in definitions.

POLICY SUBJECT:
Reporting and Investigating Privacy Breaches and Complaints

PURPOSE:
To ensure that all Privacy Breaches and Complaints involving Personal Information and/or Personal Health Information are reported, recorded, and investigated.

To prescribe the key steps in responding to Privacy Breaches and Complaints.

To ensure the relevant factors prescribed in the regulations under *The Personal Health Information Act* (PHIA) and *The Freedom of Information and Protection of Privacy Act* (FIPPA) are considered when determining if a Privacy Breach could reasonably be expected to create a real Significant Harm to an Individual or Individuals.

To comply with PHIA and FIPPA and notify Individuals affected by a Privacy Breach when a real risk of Significant Harm has been determined to have been created for those Individuals.

BOARD POLICY REFERENCE:
Executive Limitation (EL-07) Corporate Risk
Executive Limitation (EL-02) Treatment of Clients

POLICY:
Any report of a Privacy Breach, alleged Privacy Breach or Complaint shall be investigated.

The Privacy and Access Specialist shall be informed of all Privacy Breaches, alleged Privacy Breaches and Complaints; and their outcome, and shall maintain a database of this information

and analyze this information for statistical purposes and reporting to the Chief Executive Officer.

The Privacy and Access Specialist shall be informed as soon as reasonably practical where a confirmed/unconfirmed Privacy Breach involves a large number of records or heightened sensitivity.

All Staff who become aware of a Privacy Breach or risk of a Privacy Breach shall complete the ORG.1810.PL.001.FORM.01 Occurrence Report in accordance with ORG.1810.PL.001 Occurrence Reporting and Managing Critical Incidents, Critical Occurrences, Occurrences and Near Misses.

All Staff shall manage Complaints about Privacy in accordance with ORG.1810.PL.003 Complaint Management and Monitoring.

Any known or suspected Privacy Breaches involving medical staff shall be forwarded to the Privacy and Access Specialist for review and investigation.

The Privacy Officer at the Site and/or the Privacy and Access Specialist shall be responsible for communicating with contracted persons, volunteers, students, researchers, Southern Health-Santé Sud medical staff, educators, members of the Board of Directors, Information Managers or agents of any of the above or other health services agencies regarding a Privacy Breach and the findings of an investigation.

Southern Health-Santé Sud shall notify affected Individuals of a Privacy Breach if the breach could reasonably be expected to create a real risk of Significant Harm to the affected Individuals.

When notifying an affected Individual about a Privacy Breach that is reasonably expected to create a real risk of Significant Harm to the Individual, the Manitoba Ombudsman must also be notified, at the same time, and in the form and manner that the Manitoba Ombudsman requires.

DEFINITIONS:

Client: Any person (including a Person Permitted to Exercise the Rights of an Individual, where the context so requires) who receives health care services within Southern Health-Santé Sud, including patients and residents.

Complaint: A Complaint made to a Trustee or Public Body by an Individual and/or by the Provincial Ombudsman about collection, Access, correction, Use, Disclosure, protection, and Privacy of Personal Information and/or Personal Health Information.

Individual: The natural person (human being) the information is about. This includes a patient, client or resident receiving Health Care services within a Trustee. For the Access, correction,

Use and Disclosure of Personal Information or Personal Health Information includes Persons Permitted or Authorized to Exercise the Rights of an Individual.

Personal Health Information: Recorded information about an identifiable Individual that relates to:

- the Individual's health, or Health Care history, including genetic information about the Individual;
- the provision of Health Care to the Individual;
- payment for Health Care provided by the Individual;

and includes:

- the personal health identification number (PHIN) and any other identification number, symbol or particular assigned to the Individual; and
- any identifying information about the Individual that is collected in the course of, and is incidental to, the provision of Health Care or payment for Health Care;

and for further clarity includes:

- Personal information such as financial position, home conditions, domestic difficulties or any other private matters relating to the Individual which have been disclosed to the Trustee;

and for the purpose of the Confidentiality policy:

- any Personal Health Information exchanged verbally about an identifiable Individual.

Personal Information: Recorded information about an identifiable Individual, including:

- the Individual's name,
- the Individual's home address or home telephone, facsimile or e-mail number
- information about the Individual's age, sex, sexual orientation, marital or family status,
- information about the Individual's ancestry, race, colour, nationality or national or ethnic origin,
- information about the Individual's religion or creed or religious belief, association or activity,
- personal health information about the Individual
- the Individual's blood type, fingerprints or other hereditary characteristics,
- information about the Individual's political belief, association or activity,
- information about the Individual's education, employment or occupation or educational, employment or occupation history,
- information about the Individual's source of income or financial circumstances, activities or history,
- information about the Individual's criminal history, including regulatory offences,
- the Individual's own personal views or opinions, except if they are about another person,
- the views or opinions expressed about the Individual by another person, and
- an identifying number, symbol or other particular assigned to the Individual.

Persons Associated with Southern Health-Santé Sud: Includes all contracted persons, volunteers, students, researchers, Southern Health-Santé Sud medical staff, educators, members of Boards of Directors, Information Managers and employees.

Privacy: The fundamental right of an Individual to control the collection, Use and Disclosure of their Personal Information and Personal Health Information.

Privacy Breach: Means, in relation to Personal Information and Personal Health Information,

- theft or loss; or
- access, use, disclosure, destruction or alteration in contravention of *The Personal Health Information Act* or *The Freedom of Information and Protection of Privacy Act.*

Privacy Officer: An employee designated by Southern Health-Santé Sud whose responsibilities include dealing with requests from Individuals who wish to examine, receive a copy or make a correction to Personal Health Information Maintained by the Trustee and facilitating the Trustee's compliance with PHIA. The definition is intended to mean the Privacy Officer and/or their designate.

Public Body: A local Public Body such as an educational body, a health care body, and a local government body.

Significant Harm: Includes, in relation to an Individual, bodily harm, humiliation, damage to the Individual's reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the Individual's credit rating or report, and damage to or loss of the Individual's property

Site: A Health Care Facility, community health center, community office within Southern Health-Santé Sud.

Staff: includes all employees and Persons Associated with Southern Health-Santé Sud including medical staff, contracted Individuals, students, volunteers, researchers, educators, and board members.

Trustee: A health professional, a health care facility, public body or health care services agency that collects, or maintains Personal Health Information.

See also ORG.1411.PL.502.SD.01 PHIA Definitions

IMPORTANT POINTS TO CONSIDER:

- Individuals trust Staff will respect their privacy and only use personal information and personal health information about themselves as authorized under the law. Any Staff that abuse this trust by intentionally gaining access to, collecting, using or disclosing or attempting to access an Individual's personal information and/or personal health information where not permitted under PHIA or FIPPA, is guilty of an offence.
- The appropriate resources, including Human Resources, the Privacy and Access Specialist or Quality, Patient Safety and Accreditation should be consulted prior to interviewing Staff where education and/or corrective action may be required.

- If it is determined that a Privacy Breach has occurred, the manager shall consult with Human Resources and the Privacy and Access Specialist to establish the appropriate level of education and/or corrective action to be applied.
- When a Privacy Breach involving medical staff is confirmed, the Privacy and Access Specialist will consult with the facility Chief of Medical Staff and/or the Regional Lead – Medical Services and Chief Medical Officer to determine the severity of the Privacy Breach. The facility Chief of Medical Staff and/or the Regional Lead-Medical Services and Chief Medical Officer will determine the appropriate level of education and/or corrective action to be applied.
- Southern Health-Santé Sud as a trustee under PHIA and a public body under FIPPA considers the protection of personal information and personal health information to be an important and serious matter; and any Staff, who receive a Complaint about Privacy or have knowledge or suspicion of a Privacy Breach are required to immediately notify their manager, Privacy Officer or designate at the Site.
- Appropriate documentation shall be maintained during the investigative process.
- Where it has been determined there is no real risk of Significant Harm to affected Individuals, there may be other factors to consider when making the decision to notify Individuals about a Privacy Breach such as a contractual obligation or Southern Health-Santé Sud's commitment to being open and transparent.
- Reporting a Privacy Breach to Manitoba Ombudsman is viewed as a positive action and may help any Complaints investigated by Manitoba Ombudsman as a result of a Privacy Breach.

PROCEDURE:

Table of contents for procedure section:

Step 1: Report or Identification of a Privacy Breach, Alleged Privacy Breach or Complaint

1.1 Upon discovery of a Privacy Breach take immediate common-sense steps to contain or limit the breach. These steps may include:

- retrieving any documents or copies of documents that were wrongfully disclosed or taken by an unauthorized person;
- conducting physical searches for records that were lost or stolen;
- requesting and verifying that an unintended recipient double deleted all emails, correspondence and records related to the Privacy Breach;
- shutting down the system that was breached or correcting weaknesses in security;
- notifying a third-party technical company if the breach was due to a technical failure;
- revoking access to the system;
- changing passwords; and/or

- notifying Digital Health when a device, such as a laptop or smart phone is stolen or lost.

1.2 Notify law enforcement in the event of a theft or other illegal activity.

1.3 Immediately report the Privacy Breach, alleged Privacy Breach or Complaint to a manager, the Privacy Officer or designate for the Site or the Privacy and Access Specialist to investigate.

Step 2: Investigation

2.1 Identify the person who will take the lead in the investigation; a manager, the Privacy Officer or designate at the Site, or the Privacy and Access Specialist.

2.2 Decide whether or not to proceed with investigating the Complaint or alleged Privacy Breach by considering:

- if the elapsed time has made the investigation no longer practicable;
- whether the Complaint has been made in good faith; or
- whether the circumstance warrants an investigation.

2.3 Conduct fact finding and complete a preliminary report with the following information:

- date and time of the incident;
- source of report;
- incident information and description;
- Individuals affected by the incident;
- employees involved in the incident;
- security safeguards in place at the time of the incident;
- type of information and description;
- form of information (electronic, verbal, paper etc.);
- media/mode; and
- any other information pertinent to the investigation.

Note: ORG.1411.PL.203.FORM.01 Privacy Incident Report Form and ORG.1411.PL.203.FORM.02 Reporting and Investigating Privacy Breaches and Complaints – Fact-finding Interview Guide may be used for this purpose.

2.4 Determine the status of the event.

Note: A determination must be made as to whether or not a Privacy Breach occurred.

- <u>No Privacy Breach</u>
  - If the investigation is the result of a Complaint filed by an Individual, advise the Individual in accordance with ORG.1810.PL.003 Complaint Management and Monitoring that the investigation concluded no Privacy Breach occurred and of their right to make a Complaint to the Manitoba Ombudsman.
  - If the investigation is a result of an internal report, advise the Staff who reported the alleged Privacy Breach that the investigation concluded that no Privacy Breach occurred.
- <u>Unconfirmed Privacy Breach</u>
  - Consult with the Privacy and Access Specialist and provide information about the status of the investigation.

- Provide an update regarding the investigation to the complainant and/or the Staff that reported the alleged breach and assure them the organization is continuing to investigate.

➢ Confirmed Privacy Breach
- Complete a thorough assessment of the real risk of Significant Harm using Manitoba Ombudsman Practice Notes PHIA Privacy Breach Risk Rating Tool or FIPPA Privacy Breach Risk Rating Tool to determine if a real risk of Significant Harm has been created for the affected Individual(s).
- Notify the Privacy and Access Specialist.
- For Staff involved in the breach, obtain a copy of the signed Declaration of Confidentiality and confirm PHIA training via the Learning Management System (LMS) has been completed within the last three years.
- Where applicable, inform Human Resources of the Privacy Breach to discuss further investigations.
- Consult with other stakeholders, including Quality, Patient Safety and Accreditation, Digital Health or professional or other regulatory bodies.

Step 3: Notify

Notification must be provided to Individuals affected when a breach could reasonably be expected to create a real risk of Significant Harm to the Individual.

3.1 Provide notification of the Privacy Breach to the Individual in writing:

➢ as soon as practicable after the Privacy Breach becomes known to the trustee or public body;

➢ in a form and manner, and include the information, required by the regulations under PHIA and/or FIPPA and following Manitoba Ombudsman practice note Privacy Breach Notification Letter Checklist; and

➢ given directly to the Individual except in circumstances set out in the regulations, in which case it may be given indirectly in the form and manner required by the regulations (i.e. Privacy Breach of many records where it may cause a risk to public health and safety, the identity or contact information of the affected individuals is unknown, it is impracticable because of the large amount of individuals affected, or it could threaten or harm the individual's mental or physical health).

➢ Where a delay necessary to provide written notice is likely to significantly increase a real risk of Significant Harm to the Individual, the notice may be provided orally and the written notice given within a reasonable time after the oral notice is provided.

Step 4: Report

➢ Download and complete the fillable PDF FIPPA or PHIA Privacy Breach Reporting Form found on Manitoba Ombudsman's website Privacy Breach Resources - Manitoba Ombudsman. Do not include any identifiable personal or personal health information.

➢ Submit the form by email at omudsman@ombudsman.mb.ca or fax at 204-942-7803.

Step 5: Prevent Future Breaches

5.1 Undertake a thorough analysis of the cause and extent of the breach. This may include a security audit of physical, technical and administrative safeguards.

5.2 Implement long-term safeguards against further breaches such as providing on-going education and training to staff about PHIA and FIPPA; changing policies, procedures and practices; and corrective actions.

5.3 Work in collaboration with the Privacy and Access Specialist to perform audits on any long-term safeguards implemented, as a result of the Privacy Breach, to ensure that the prevention plan is successful.

SUPPORTING DOCUMENTS:

ORG.1411.PL.203.FORM.01 - Privacy Incident Report Form

ORG.1411.PL.203.FORM.02 - Reporting and Investigating Privacy Breaches and Complaints – Fact-finding Interview Guide

REFERENCES:

ORG.1411.PL.001.SD.01 FIPPA Definitions

ORG.1411.PL.502.SD.01 *The Personal Health Information Act* (PHIA) Definitions

ORG.1512.PL.001 Discipline and Notice of Discharge

The Personal Health Information Act (Manitoba), S.M. 1997, c. 51

The Freedom of Information and Protection of Privacy Act (Manitoba) S.M. 1997, c. 50

Shared Health Reporting and Investigating Privacy Breaches and Complaints Policy 340.100.100

Manitoba Ombudsman Privacy Breach Resources – https://www.ombudsman.mb.ca/info/privacy-breaches.html