CancerCare Manitoba
ActionCancerManitoba

GOVERNING DOCUMENTS

Policy and Procedure

Title:	**Reporting and Investigating Privacy Breaches and Complaints** *(Previously: Reporting of Security Breaches Related to Personal Health Information and the Corrective Procedures to be Followed)*
Policy Number:	06.028 *(Previously 02.009)*
Effective Date:	October 21, 2011
Revised Date:	September 23, 2015
Approving Body:	President and CEO
Authority:	CancerCare Manitoba Act
Responsible Officer:	President and CEO
Delegate:	
Contact:	Health Information Services and Privacy Officer
Applicable to:	CCMB Staff and Physicians

1.0 BACKGROUND:

Not Applicable

2.0 PURPOSE:

2.1 To ensure that all Privacy Breaches and Complaints involving Personal Health Information are reported, recorded and investigated.

2.2 To prescribe the process for investigating Privacy Breaches and Complaints.

2.3 To establish procedures for implementing corrective actions and to minimize the risk of additional Privacy Breaches.

3.0 DEFINITIONS:

3.1 **Complaint:** A Complaint made to a Trustee by any person alleging a Privacy Breach.

3.2 **Health Care Facility:** A hospital, personal care home, Psychiatric Facility, medical clinic, Laboratory, CancerCare Manitoba, community health centre or other facility in which Health Care is provided and that is designated in the regulations under PHIA.

3.3 **Individual:** A patient or client receiving, or who has received, health care services within a CCMB Facility.

3.4 **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; or
- Payment for health care provided to the Individual;

and includes:

- The PHIN (personal health identification number) and any other identification number, symbol or particular assigned to an 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
- Any Personal Health Information exchanged verbally about an identifiable Individual.

3.5 **Persons associated with CCMB:** includes all contracted persons, volunteers, students, researchers, WRHA medical staff, educators, members of the Boards of Directors, Information Managers, employees, or agents of any of the above.

3.6 **PHIA:** *The Personal Health Information Act (Manitoba)*

3.7 **Privacy Breach:** is the result of an unauthorized access, collection, use or disclosure of Personal Health Information in violation of *The Personal Health Information Act,* or the integrity or security of the information is in some way compromised.

3.8 **Privacy Office:** An employee designated by CancerCare Manitoba whose responsibilities may include dealing with requests from Individuals who wish to examine and copy or to correct Personal Health Information collected and maintained by the Trustee and facilitating the Trustee's compliance with PHIA. At CancerCare Manitoba, the Medico-Legal correspondent assists the Privacy Officer in this designated capacity.

3.9 **Record or Recorded Information:** A record of information in any form, and includes information that is written, photographed, Recorded or stored in any manner, on any storage medium or by any means, including by graphic, electronic or mechanical means, but does not include electronic software or any mechanism that produces Records.

3.10 **Security:** The process of protecting the Personal Health Information by assessing threats and risks to information and taking steps to mitigate these threats and risks. The result is the consistent application of standards and controls to protect the integrity and privacy of the information during all aspects of its use, processing, disclosure, transmittal, transport, storage, retention including conversion to a different medium and destruction.

3.11 **Trustee:** A health professional, Health Care Facility, public body, or health services agency that collects or maintains Personal Health Information.

3.12 **Incident Reporting Database:** A database utilized within CCMB to record, track, trend events for purposes of organizational learning and identifying opportunities for system improvements.

4.0 **POLICY:**

4.1 Any Persons Associated with CCMB who have received a Complaint, or who have knowledge of a Privacy Breach or reasonable suspicion of a Privacy Breach, shall immediately notify their Manager or Privacy Office.

4.2 The Manager shall consult with the Patient Representative and Privacy Office to determine whether investigating the Complaint or possible Privacy Breach is required. In determining whether to proceed with an investigation, the Manager, Patient Representative and/or Privacy Office shall consider:

- If the elapsed time has made the investigation no longer practicable;
- Whether the Complaint has been made in good faith; and
- Whether the circumstance warrants an investigation.

4.3 Where the initial investigation reveals that a confirmed/unconfirmed Privacy Breach requires additional investigation, the Privacy Office, Patient Representative and Manager shall determine who will take the lead on the investigation and will consult with Human Resources. The Privacy Office shall immediately inform the Executive Office where the confirmed/unconfirmed Privacy Breach involves a large number of Records or heightened sensitivity.

4.4 In accordance with Section 5.6 of this policy, all confirmed Privacy Breaches must be documented in the Incident Reporting database by the Manager, Patient Representative or Privacy Office conducting the investigation.

5.0 **PROCEDURE:**

5.1 The Manager, Patient Representative and/or the Privacy Office shall conduct the initial investigation, which may include:

- Identification of the Persons Associated with CCMB involved;
- Identification of the Personal Health Information in question;
- The nature and extent of the alleged Privacy Breach;
- Gathering relevant documents;
- Consulting with the appropriate resources, including Legal, Human Resources and/or the Executive prior to interviewing staff where there may be potential disciplinary consequences; maintain appropriate documentation.

5.2 Based on the findings of the initial investigation, the Manager, Patient Representative and/or Privacy Office shall determine the status of the event to be one of the following:

- No Privacy Breach;
- Unconfirmed Privacy Breach; or
- Confirmed Privacy Breach.

5.3 Where the initial investigation reveals:

5.3.1 No Privacy Breach: If the investigation ensued as a result of a Complaint filed by an Individual, the Manager, Patient Representative and/or Privacy Office must advise the Individual(s) that the investigation determined no Privacy Breach occurred and they have a right to make a Complaint to the Manitoba Ombudsman.

5.3.2 Unconfirmed Privacy Breach: The Manager, Patient Representative and/or Privacy Office may, at the discretion of the Privacy Office notify the Executive Office and the Individual(s) affected, provide an explanation and advise that further investigation is underway.

a) If the unconfirmed Privacy Breach is later determined to be a confirmed Privacy Breach, the process in 5.3.3 of this policy must be followed.
b) If it is determined that no Privacy Breach has occurred, the process in 5.3.1 of this policy must be followed.

5.3.3 Confirmed Privacy Breach: The Manager, Patient Representative and/or Privacy Office, shall notify the Executive of the breach. They may notify the Individual(s) affected, make an apology on behalf of the organization, and advise them of their right to make a Complaint to the Manitoba Ombudsman.

a) Take immediate steps to contain the Privacy Breach by stopping the unauthorized practice; recover the Records; shut down the system that was breached; revoke access or correct weaknesses in physical Security.
b) The Privacy Office shall obtain a copy of the signed PHIA Pledge of Confidentiality for the Person Associated with CCMB and confirm PHIA training has been conducted.
c) Any alleged breaches of this Policy involving physicians shall initially be investigated and processed in accordance with this Policy. Should a physician be found to be in breach of this Policy appropriate disposition shall occur in consultation with the Chief Medical Officer (CMO).This disposition does not prevent the simultaneous referral of the issue by the CMO as a “complaint” pursuant to Section 8 of the Medical Staff By-law. The CMO may determine the appropriate disposition of the complaint, in accordance with the Medical Staff By-law, and whether the physician’s privileges should be affected. Physician privileges can only be affected through the By-law processes in the Medical Staff By-law.
d) The Manager, Patient Representative and Privacy Officer shall

inform Human Resources of the privacy breach and discuss further investigation options.

e) The Manager and Human Resources will expand the investigation to include employee interviews and determine if the Privacy Breach is a culpable or non-culpable Privacy Breach or a systemic breach.

5.4 Where a confirmed Privacy Breach is determined to be culpable:

5.4.1 The Privacy Office in consultation with Human Resources will determine the severity of the Privacy Breach.

5.4.2 The Manager in consultation with Human Resources will determine the disciplinary action to be taken.

5.4.3 The Manager, Patient Representative and/or Privacy Office in consultation will send a final letter to Individual(s).

5.4.4 Where a Privacy Breach involves a physician, the process outlined in 5.4.1, 5.4.2, and 5.4.3 will be conducted by the CMO office and liaise with the Privacy Office.

5.5 Where a confirmed Privacy Breach is determined to be a non-culpable or systemic Privacy Breach; the Privacy Office shall ensure the issue is rectified and/or make recommendations to the Department/Unit/Manager in a timely manner.

5.6 For culpable and non-culpable or systemic Privacy Breaches, the Manager, Patient Representative, Privacy Office shall document the details of the Privacy Breach, the subsequent investigation and the corrective actions taken in the Incident Reporting database.

5.7 The Privacy Office may prepare an annual Privacy Breach summary report for Executive.

5.8 The Executive may, on an annual basis, prepare a regional Privacy Breach summary report for the Board.

6.0 **REFERENCES:**

6.1 WRHA Reporting and Investigating Privacy Breaches and Complaints, Policy 10.40.110

6.2 *The Personal Health Information Act*

6.3 *The Personal Health Information Act Regulations*

6.4 Privacy Breach Investigation Process Chart
http://home.wrha.mb.ca/privacy/files/PrivacyBreach-InvestigationProcess.pdf

Policy Contact: All enquiries relating to this policy should be directed to:	
Name:	Venetia Bourrier
Title/Position:	Director, Health Information Services and Privacy Officer
Phone:	204-787-2158
E-mail:	vbourrier@cancercare.mb.ca
Address: (if required):	

DOCUMENTATION	
Policy Location: This policy is located (hard and e-copy formats):	
1.	The original signed and approved policy is on file in the Executive Office, CCMB
2.	The e-copy is on file in the CCMB Governing Documents Library, SharePoint
3.	

Revision History:

Date	Version	Status	Author	Summary of Changes
dd/mm/yyyy	#	Initial, Draft Final Minor/Major revision		
21/10/2011	1	Initial		
23/09/2015	2	Minor Revision	L Costa Policy Team	Revisions made to reflect current WRHA policy.
05/04/2018	2	Minor revision	S.Friedenberger	Reformatted to new template

Approvals Record:
This Policy requires approval by:

Approval		
Date	**Name / Title**	**Signature**
	Not required.	

FINAL APPROVAL:

Date	**Name / Title**	**Signature**
Oct 29 2015	Dr. S. Navaratnam President and CEO, CCMB	*Original signed by* *Dr. S. Navaratnam*