CATEGORY:	**ORGANIZATIONAL: INFORMATION MANAGEMENT**
SUB-CATEGORY:	**PRIVACY**
GROUP:	
DISTRIBUTION:	**ALL EMPLOYEES**
TITLE:	**PRIVACY BREACH MANAGEMENT**

PURPOSE

To provide a consistent and effective approach to the investigation and management of privacy breaches involving personal information / personal health information.

POLICY

It is the responsibility and obligation of all employees, physicians, agents, contractors, volunteers students and those health care professionals who have the right to treat persons at a health care facility operated by Western Health to ensure that information to which they have access is kept confidential and private.

Western Health must respond to all privacy breaches as defined in this policy. All privacy breaches must be reported to the immediate manager of the department/program as well as the Regional Manager, Information Access and Privacy or designate.

The configuration of the physical facilities of Western Health may limit the capacity to ensure complete privacy of personal health information in the process of providing care/service. Nonetheless, all reasonable efforts must be made to avoid preventable privacy breaches within the constraints of the care/service delivery environment.

This includes information that is:

- in any format including, but not limited to, paper, electronic, film, visual and/or verbal discourse,
- provided to, obtained from, or as a result of a relationship with Western Health, regardless of where that information may be subsequently stored or used.

In the event of a privacy breach, employees, physicians, agents, contractors, volunteers students and those health care professionals who have the right to treat persons at a health care facility operated by Western Health must:

1. **Immediately** notify the manager /leader in their program/department.

The manager/director must immediately:

1. Ensure that the appropriate employee completes an *Occurrence Report* in keeping with Western Health's *Occurrence Reporting* policy (6-02-15).

2. Consult with the Regional Manager, Information Access and Privacy or designate to assist in:

   a. identifying the level of the incident and take appropriate action to contain the breach (i.e. by stopping the unauthorized practice, recovering the information, changing password, assessing lost or stolen equipment that may contain confidential information (e.g. laptop, fax machine);

   b. assessing the risks associated with the breach (i.e. the type of information involved, who was affected, number of individuals affected, assessing whether information can be used for fraudulent or harmful purposes);

   c. determining if there is a risk of ongoing or further exposure;

   d. determining whether Human Resources personnel are required to be involved in the investigation or whether the engagement of Medical Services is required under the Medical Staff bylaws. (Willful breaches may result in disciplinary action, up to and including termination of employment or contract/service);

   e. identifying the circumstances that caused the incident and reporting on the investigation of the incident;

   f. determining follow-up actions required to prevent further breaches of a similar nature; and

   g. ensuring that the *Client Feedback: Compliments and Complaints* policy (6-04-60) is followed where applicable. This applies in cases where the affected client / patient / resident wishes to submit a complaint to Western Health, either instead of or in addition to being provided the contact information for the Office of the Information and Privacy Commissioner (OIPC) for the province.

In consultation with the Regional Director Quality and Risk Management or designate as required, the Regional Manager, Information Access and Privacy or designate must:

1. Determine appropriate managers/directors/senior leaders, to be notified.

2. Where the privacy incident involves an individual other than an employee or healthcare provider of Western Health (i.e. student, healthcare provider, pastoral care, and contractor), assist in the investigation with the manager/director and/or entity.

3. Consult with appropriate managers/directors/senior leaders, as required to:
   a. identify other stakeholders requiring notification of the incident:
      - internal stakeholders such as: Communications, Information Management, Human Resources, Employee Assistance Program;
      - The Department of Health and Community Services in keeping with the provincial *Regional Health Authority Privacy Auditing, Reporting, and Public Notification policy*;
      - Law enforcement, if theft or other crimes are suspected;
      - Media;
      - Western Health's solicitor (to discuss contractual and/or other legal obligations);
        - Insurers and others – if required by contractual obligations;
        - Professional or other regulatory bodies;
        - Contractual obligation and legal requirements for notification.

   b. provide notification to the OIPC and Access to Information and Protection of Privacy (ATIPP) Office as required in keeping with policy *Duty to Notify the Office of the Information and Privacy Commissioner of a Breach* (9-03-20);

   c. determine and provide direction with respect to whether to notify affected individuals (e.g. contractual obligations, risk of identity theft, risks associated with loss of information) in keeping with policy *Duty to Notify an Individual of a Privacy Breach* (9-03-30);

   d. identify and provide direction with respect to how affected individuals affected will be notified (i.e. direct notification or in exceptional circumstances, indirect notification);

   e. determine and provide direction with respect to the level of information to be disclosed during notification (i.e., date of breach, description of breach, description of information inappropriate accessed/collected/disclosed, steps taken to mitigate the harm, contact information of the OIPC);

f. determine and provide direction with respect to the level of expertise required to assist in the notification (e.g. to address any technical questions, assess if the individual is at risk of harm to self or others);

4. Complete:
   i) the appropriate Privacy Breach Reporting form as required by the OIPC and /or Access to Information and Protection of Privacy (ATIPP) Office within the Department of Justice and Public Safety,
   ii) as required, a Briefing Note and forward it to the Chief Executive Officer.

5. Consult with the Regional Director of Communications as required.

6. Where notification takes place via telephone, ensure follow up with written documentation directed to the client/patient/resident in keeping with the *Disclosure of Occurrences* policy (6-02-16).

7. Where appropriate, ensure that a copy of the notification letter is placed on client's health record.

8. Review results of investigation and develop an action plan to improve adequate long term safeguards against further breaches (address administrative, physical or technical issues):
   - determine if a security audit of both physical and technical security is required;
   - review policies and update them to reflect lessons learned from the investigation;
   - audit at the end of the process to ensure that the prevention plan and corrective actions have has been fully implemented;
   - address any further staff training needs with respect to the organization's privacy obligations under applicable legislation.

9. Cooperate and collaborate with the OIPC and/or Access to Information and Protection of Privacy (ATIPP) Office within the Department of Justice and Public Safety in any further investigation into the privacy incident and address any recommendations that are forthcoming.

10. Collaborate with the manager/director and Risk Management to ensure occurrence report outlines events of investigation, outcome and recommendations.

11. Maintain all relevant information such as status reports, e-mails, relevant documents, briefing notes and recommended changes, auditing measures.

DEFINITIONS

Confidentiality: An obligation to keep an individual's personal health information private, ensuring that those authorized have access to the information.

Direct notification: Refers to notifying individuals who have been affected by a privacy breach through direct means including telephone, letter or in person.

Disclose: To make the information available or to release it but does not include a use of the information and "disclosure" has a corresponding meaning.

Indirect notification: Refers to notifying individuals who have been affected by a privacy breach through indirect means including website information, posted notices, or the media.

Personal health information: Identifying information in oral or recorded form about an individual that relates to:

- information concerning the physical or mental health of the individual, including information respecting the individual's health care status and history and the health history of the individual's family;
- the provision of health care to the individual, including information respecting the person providing the health care;
- the donation by an individual of a body part or any bodily substance, including information derived from the testing or examination of a body part or bodily substance;
- registration information;
- payments or eligibility for a health care program or service in respect of the individual, including eligibility for coverage under an insurance or payment arrangement with respect to health care;
- an individual's entitlement to benefits under or participation in a health care program or service;
- information about the individual that is collected in the course of, and is incidental to, the provision of a health care program or service or payment a health care program or service;
- a drug as defined in the *Pharmacy Act*, a health care aid, device, product, equipment or other item provided to an individual under a prescription or other authorization issued by a health care professional; or
- the identity of a person's representative as defined in Section 7 of the *Personal Health Information Act*.

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

(i) the individual's name, address or telephone number,
(ii) the individual's race, national or ethnic origin, colour, or religious or political beliefs or associations,
(iii) the individual's age, sex, sexual orientation, marital status or family status,
(iv) an identifying number, symbol or other particular assigned to the individual,

(v) the individual's fingerprints, blood type or inheritable characteristics,
(vi) information about the individual's health care status or history, including a physical or mental disability,
(vii) information about the individual's educational, financial, criminal or employment status or history,
(viii) the opinions of a person about the individual, and
(ix) the individual's personal views or opinions, except where they are about someone else.

Privacy: The right of individuals to control the collection, use and disclosure of information about themselves.

Privacy breach: A privacy breach occurs when there is unauthorized and/or inappropriate access, collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of the *Access to Information and Protection of Privacy Act* (*ATIPPA*) or the *Personal Health Information Act* (*PHIA*.) The most common privacy breaches occur when personal information of clients, patients, residents, employees or a corporation is stolen, lost, mistakenly disclosed or inappropriately accessed. For example, a privacy breach occurs when a computer/laptop containing personal information is stolen or personal information is mistakenly emailed or faxed to the wrong person.

LEGISLATIVE CONTEXT

Access to Information and Protection of Privacy Act, 2015. Available at: http://www.assembly.nl.ca/legislation/sr/statutes/a01-2.htm

Personal Health Information Act (2008). Available at: http://www.assembly.nl.ca/legislation/sr/statutes/p07-01.htm

REFERENCES

Central Health (2013). *Privacy Breach Management*

Government of Newfoundland and Labrador, ATIPP Office, Protection of Privacy, Privacy Breach Protocol, March 2015

Newfoundland and Labrador *Personal Health Information Act*, Policy Development Manual, Version 1.2, February 2011

Newfoundland and Labrador Health and Community Services, Regional Health Authority Meditech Privacy Auditing, Reporting, and Public Notification Policy (Version 1.0), May 1, 2013.

Newfoundland and Labrador Health and Community Services, *Personal Health Information Act*, Privacy Breach Guidelines for Custodians of Personal Health Information, Risk Management Toolkit, April 30, 2010.

Office of the information and Privacy Commissioner Newfoundland and Labrador. Avoiding Inadvertent Privacy Breaches – Quick Tips. Available at: http://www.oipc.nl.ca/pdfs/Avoiding_Inadvertant_Breaches_Tip_Sheet.pdf

KEY WORDS

Breach, breach of privacy, privacy, privacy breach, confidentiality

TO BE COMPLETED BY STAFF IN QUALITY DEPARTMENT

Approved By: Chief Executive Officer	Maintained By: Regional Manager, Information Access & Privacy
Effective Date: 18/March/2009	☑ Reviewed: 16/July/2018 ☑ Revised:
Review Date: 16/July/2021	☐ Replaces: *(Indicates name and number of policy being replaced)* OR New