Approval Date	*July 8, 2021*
Revision Date	*March 20, 2011, May 10, 2013, January 20, 2021.*
Approved by	*Andree Robichaud, CEO*
Approver Signature	
Scheduled Review Date	*July 2024*
Cross- Reference	*4-g-10 Privacy Breach*

PURPOSE

The purpose of this policy is to ensure that policy and procedure is followed in responding to breaches of privacy or security.

SCOPE

This policy applies to all Central Health employees and affiliated individuals, including trustees, volunteers, pastoral care providers, contractors, vendors, students, etc.

This policy applies to any confidential information in any format, including personal; personal health; and/or business information of Central Health not otherwise available publicly and gained through affiliation with Central Health.

DEFINITIONS

Affiliated Individuals	Individuals who are not employed by Central Health, but perform specific tasks at or for the organization, including, but not limited to, trustees, students, volunteers, pastoral care, researchers, contractors, vendors and individuals working at the organization, but funded through an external source.
Business Information	Information with respect to Central Health's business that is not publicly disclosed by the organization. Employees / affiliates may come in contact with such information that is not generally known to the public as they perform their

	duties. Examples include, but are not limited to: • legal matters involving the organization that are not public knowledge; • financial information that is not available in Central Health's annual report; • contractual agreements with vendors, consultants, contractors, and third parties (The confidentiality of this information may be written into the contract, e.g. non-disclosure of the cost of the service); • information about intellectual property such as development of new technology and treatments or unpublished reports; and • information pertaining to Central Health's information technology access and systems.
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: • 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 for a health care program or service; • a drug as defined in the *Pharmacy Act, 2012*, 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: • the individuals name, address, or telephone number; • the individual's race, national or ethnic origin, color, or religious or political beliefs or associations; • the individual's age, sex, sexual orientation, marital status or family status; • an identifying number, symbol or other particular assigned to the individual; • the individual's fingerprints, blood type or inheritable characteristics; • information about the individual's health care status or history, including a physical or mental disability; • information about the individual's educational, financial, criminal, or employment status or history; • the opinions of a person about the individual; and • the individual's personal views or opinions.
Privacy Breach	A privacy breach occurs when there is unauthorized and/or inappropriate access, collection, use, disclosure or disposal of personal/personal health or business information. Such activity is "unauthorized" if it occurs in contravention of

	ATIPPA or *PHIA*. The most common privacy breaches occur when personal information of clients, employees or a corporation is stolen, lost or mistakenly disclosed. 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.

POLICY STATEMENT(S)

All individuals are accountable to ensure the confidentiality of information and protection of privacy of individuals who are the subject of information entrusted to our care.

It is the responsibility and obligation of all health care professionals/providers, employees, trustees, students, volunteers, contractors and any other affiliated individual engaged by Central Health to ensure that information to which they have access is kept confidential and private. Central Health must respond to all privacy breaches, accidental or intentional.

Privacy breaches may result in disciplinary action, up to and including termination of employment or contract/service.

All privacy breaches must be reported through the Central Health Clinical Safety Reporting System (CSRS), as well as to the manager/director of the department/program, in consultation with the Central Health Privacy Manager as required.

PROCEDURE

In the event of a privacy breach, all individuals are accountable to **immediately** notify the manager/director or designate.

A CSRS occurrence report must be **immediately** entered by any individual who becomes aware of a potential privacy incident.

The Manager/Director must:

1. Consult with the Privacy Manager to discuss the specifics of the incident and the response protocol to follow to ensure appropriate action is taken to contain and respond to the situation;
2. In consultation with Privacy Manager, take all necessary steps to prevent further compromise of the information; i.e. retrieval of the compromised records from the unauthorized recipient, change password, assess lost or stolen equipment that may contain confidential information (i.e., laptop, fax machine, etc.);
3. Consult with the Privacy Manager to determine if Talent and Culture personnel need to be involved in the investigation of the privacy breach or whether the engagement of medical services is required under medical staff bylaws;
4. Ensure that an Occurrence Report is completed as per Occurrence Reporting Policy;
5. Work with the Privacy Manager to investigate the circumstances of the breach,
6. Initiate, coordinate, and report on the investigation of the incident;
7. Determine follow-up actions to be implemented to prevent further breaches of a similar nature.

The Privacy Manager must:

1. Immediately implement the Provincial Privacy Breach Protocol;
2. Where indicated, in consultation with Senior Leadership, complete a 'Privacy Breach Reporting' form and forward it to the Access to Information and Protection of Privacy Office of the Department of Justice and/or Information and Privacy Commissioner of Newfoundland & Labrador;
3. Forward copy of Privacy Breach Reporting form to Chief Executive Officer;
4. When the privacy breach involves someone other than a Central Health employee or physician associated with Central Health (e.g., a student or contractor) initiate the investigation with the appropriate entity associated with the individual**;**
5. In consultation with Senior Leadership (if indicated) determine who

from the appropriate department/program area will notify those affected by the incident via direct notification or in exceptional circumstances, indirect notification;

6. In consultation with Senior Leadership determine if public disclosure or reporting to the police is required.

REFERENCES

Access to Information and Protection of Privacy Act, Statutes of Newfoundland and Labrador (2002, c. A-1.1). Retrieved from House of Assembly website: https://www.assembly.nl.ca/legislation/sr/statutes/a01-2.htm

Key Steps When Responding to a Privacy Breach, 2008, Access to Information and Protection of Privacy Office, Department of Justice.

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

Personal Health Information Act, Statutes of Newfoundland and Labrador (2008, c. P-7.01). Retrieved from House of Assembly website: https://assembly.nl.ca/legislation/sr/statutes/p07-01.htm

Privacy Breach Guidelines, Newfoundland and Labrador Health and Community Services, *The Personal Health Information Act,* Risk Management Toolkit.

Privacy Breach Notification Assessment Tool, 2008, Access to Information and Protection of Privacy Office, Department of Justice.

RESOURCES

Provincial Privacy Breach Protocol