

SUBJECT**Privacy Breach Policy**

NOTE: This is a joint policy of the Chief Privacy Officers' Working Group and shall not be modified except by agreement of that group.

INTRODUCTION

Each of the Regional Health Authorities (RHAs), FacilicorpNB, and Ambulance NB, as health system partners (herein referred to as "the Partners"), is committed to collecting, using, disclosing and disposing of personal information (PI) and personal health information (PHI) entrusted to us in a manner that is accurate, confidential, secure and private.

OBJECTIVE

The purpose of this Policy is to outline the procedures to be followed when responding to a suspected or actual privacy breach.

SCOPE

This Policy applies whenever the Partner's employees or non-staff personnel are engaged in activities where such individuals have access to PI or PHI, and a breach is suspected or occurs.

**LEGISLATIVE
REQUIREMENTS**

- *Personal Health Information Privacy and Access Act (PHIPAA)*
- *Right to Information and Protection of Privacy Act (RTIPPA)*

DEFINITIONS

"non-staff personnel" includes, but is not limited to, agents, board members, students, volunteers, physicians, consultants, third-party service providers, external professionals or experts contracted to offer a service and vendors, demonstrating, installing or servicing equipment, software applications or hardware.

"personal health information" means identifying information about an individual in oral or recorded form if the information:

- (a) relates to the individual's physical or mental health, family history or health care history, including genetic information about the individual,
- (b) is the individual's registration information, including the Medicare number of the individual,
- (c) relates to the provision of health care to the individual,
- (d) relates to information about payments or eligibility for health care in respect of the individual, or eligibility for coverage for health care in respect of the individual,
- (e) 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 body part or bodily substance,

- (f) identifies the individual's substitute decision maker, or
- (g) identifies an individual's health care provider.

"personal information" means recorded information about an identifiable individual, including but not limited to,

- (a) the individual's name,
- (b) the individual's home address or electronic mail address or home telephone or facsimile number,
- (c) information about the individual's age, gender, sexual orientation, marital status or family status,
- (d) information about the individual's ancestry, race, colour, nationality or national or ethnic origin,
- (e) information about the individual's religion or creed or religious belief, association or activity,
- (f) personal health information about the individual,
- (g) the individual's blood type, fingerprints or other hereditary characteristics,
- (h) information about the individual's political belief, association or activity,
- (i) information about the individual's education, employment or occupation or educational, employment or occupational history,
- (j) information about the individual's source of income or financial circumstances, activities or history,
- (k) information about the individual's criminal history, including regulatory offences,
- (l) the individual's own personal views or opinions, except if they are about another person,
- (m) the views or opinions expressed about the individual by another person, and
- (n) an identifying number, symbol or other particular assigned to the individual.

A **"privacy breach"** occurs when there is an unauthorized or strong potential for an *unauthorized*

- access to
- collection
- use,
- disclosure of,
- disposal of

personal information (PI) or personal health information (PHI).

POLICY STATEMENT

The Partners undertake to respond to any suspected or actual privacy breach in a timely fashion in accordance with the procedure outlined in this Policy document.

Any person suspecting a breach must immediately notify their supervisor and the Chief Privacy Officer of their organization.

PROCEDURES

There are **five** steps to follow when responding to a privacy breach:

1. Breach containment and initial investigation;
2. Internal notification/Implementing the Privacy Breach Policy;
3. Risk assessment;
4. Notification of affected individuals and others;
5. Corrective measures to prevent future breaches & Employee and Non-staff Personnel Follow-up.

Note: Steps one and two may happen simultaneously.

Step One: Breach Containment and Initial Investigation

Breach Containment

Individuals who are responsible for, or who discover an actual or suspected breach, in consultation with their supervisor and the CPO as required, shall take immediate steps, as appropriate, to contain the breach. This could include for example:

- stop the unauthorized practice,
- recover the records and **all** copies,
- shut down the system that was breached,
- revoke or change computer access codes and/or correct weaknesses in physical or electronic security,
- the supervisor should contact the Human Resources Department (HR) to discuss whether the situation merits disciplinary action.

Initial Investigation

Upon being notified of a suspected or actual breach, the CPO, in consult with the Supervisor, shall immediately undertake an investigation to determine whether a breach has occurred and the scope of the PI AND PHI compromised.

The investigation may also require:

- Consulting with external resources, where and when appropriate.
- Identifying the individuals, both internal and external, who must be made aware of the breach and that the investigation is underway.
- Notifying the police, if a breach appears to involve theft or other criminal activity
- Gathering and preserving all evidence relating to the breach. This will include the following:
 - o Determining the scope of the breach;
 - o Preserving the PHI in question;
 - o Interviewing and securing written statements and/or notes of individuals with information relevant to the breach;
 - o Obtaining all copies of all relevant documentation (written, electronic or recordings);
 - o Documenting any procedures or practices of parties involved that do not appear in writing.

Step Two: Internal Notification/Implementing the Privacy Breach Policy

- Staff must immediately notify their supervisor of an actual or suspected privacy breach. In the event that a supervisor is not available staff may contact the CPO directly.
- The Supervisor shall immediately notify the Chief Privacy Officer (CPO) for their organization. Depending on the nature or seriousness of the suspected privacy breach, the CPO will determine the additional staff to be notified, including whether or not the situation merits advising their senior executives.

- Where appropriate, the CPO of the affected Partner will notify the CPO of the Department of Health of the privacy breach, at their earliest convenience;
- The CPO will provide preliminary notification to the Access to Information and Privacy Commissioner of the breach, as appropriate.
- If a person working in one organization becomes aware of a breach or potential breach occurring in another Partner organization, they will immediately contact their CPO, who will contact the CPO for the implicated organization.

Step Three: Risk Assessment:

The CPO, in consultation with employees as required, shall immediately assess the cause and extent of the breach, and the potential harm to the affected individual(s) and others resulting from the breach.

Step Four: Notification of Affected Individuals and Others:

All privacy laws require that organizations be “transparent” in how they conduct their business. In a breach situation, we must be no less transparent in identifying what has happened. This also means that, depending on the situation and where recommended, we must notify various individuals that a breach occurred, including the individual (s) whose privacy has been determined to have been breached.

Steps for Notification:

- Determine, in consult with the communications department, if, when and how to notify (direct mail and/or phone, public notice, media, internet).
- Determine who should contact or send notification to the individuals.
- Determine what should be included in the notification.
- Prepare public notification, as appropriate.

The CPO will notify the Access to Information and Privacy Commissioner, as required.

Step Five: Corrective Measures to Prevent Future Breaches & Employee and Non-staff Personnel Follow-up

Once the investigation is complete, the CPO shall submit a report of the investigation to senior executives. The report shall include *recommendations* for corrective measures with a view to the prevention of future breaches, which may include:

- An audit of the technical and physical security
- A review of policies and procedures and recommended revisions to reflect the lessons learned from the investigation
- A review of employee training practices and recommendations as appropriate
- A review of the existing practices of service delivery partners and agents to aid in determining if corrective measures or improvements are required
- Any other measures considered by the CPO to be appropriate in the

circumstances

Employee and Non-staff Personnel Follow-up

Employee

Table “A”, the *Privacy Violations and Possible Disciplinary Actions* identifies the progressive nature of the discipline involved in the course of dealing with persons involved in a breach. It must be **noted** that the **degree of discipline** in each situation *will be determined on a case by case basis*, taking all relevant factors and circumstances into account.

In addition to possible discipline internally, an individual could be subject to legal penalties for a violation of provincial privacy legislation. This is a Category F offense under the *Provincial Offenses Procedure Act* (POPA).

Non-Staff Personnel

Managers of non-staff personnel will provide the appropriate follow-up and communicate the results to the CPO.

Table “A”: Privacy Violations and Possible Disciplinary Actions

The following levels of violations can be used as a guide when determining the actions to be taken following a founded breach of personal health information (PI AND PHI)

Levels of Privacy Violation	Examples of Violations	Possible Disciplinary Action(s)
<u>Level 1 - Unintentional</u> Carelessness in handling PI AND PHI or maintaining adequate security levels	□ Disclosing PI AND PHI without verifying identity of requestor □ Leaving PI AND PHI unattended or in public area □ Failing to log off computer that holds PI AND PHI □ Inadvertently sending PI AND PHI via fax to an incorrect fax number □ Unauthorized access of your own PI AND PHI or that of a family member	□ Discussion of applicable policies and procedures □ Privacy training and/ or letter of expectation □ Sign or re-sign confidentiality declaration □ Documented verbal or written reprimand □ In exceptional circumstances, disciplinary action as appropriate up to and including suspension with or without pay and possible dismissal.

<u>Level 2 – Intentional, non-malicious</u> Breaching policies or legislation surrounding the use and disclosure of PI AND PHI	□ Accessing PI AND PHI without professional need to know □ Discussion of PI AND PHI with someone who does not have a legitimate need to know □ Allowing another individual to use your computer account or password □ Recurrence of an unauthorized access of your own PI AND PHI or that of a family member □ Repeated Level 1 violations	□ Discussion of applicable policies and procedures □ Privacy training and/or letter of expectation □ Sign or re-sign confidentiality declaration □ Disciplinary action as appropriate up to and including suspension with or without pay and possible dismissal
<u>Level 3 – Intentional and malicious</u> Knowingly breaching policies or legislation surrounding the use and disclosure of PI AND PHI for personal gain or to harm another person(s)	□ Accessing PI AND PHI without professional need to know for personal gain or to cause harm to another(e.g.: using information for custody battle or divorce proceedings) □ Using another employee's computer account for personal gain or to cause harm to another □ Intentionally altering data or removing PI AND PHI in any form □ Repeated Level 1 or 2 violations	□ Disciplinary action - suspension without pay or dismissal (employee ineligible for future rehire) □ Revocation of Medical Staff privileges and access privileges removed

ACCOUNTABILITIES

Chief Privacy Officer is responsible to:

- Maintain current policies, standards, procedures, guidelines and tools required to support effective identification and management of privacy breaches;
- Implement, interpret and promote compliance with this policy.
- Document the results of privacy breach investigations;
- Establish processes to promptly and regularly report privacy breaches and the results of any investigation to the CEO;
- Monitor the resolution of breaches and corrective action.

Employee and Non-staff Personnel are responsible to:

- Report a potential privacy or security risk, to facilitate prevention of a breach;

- Report a suspected or actual breach to their supervisor and CPO;
- Assist with the investigation, as required; and
- Follow-up on identified privacy or security risks to enhance privacy.

REFERENCES AND ASSOCIATED DOCUMENTS

- *Personal Health Information Privacy and Access Act, (PHIPPA)*;
- *Right to Information and Protection of Privacy Act (RTIPPA)*
- Privacy Breach Tool Kit

INQUIRIES

For more information on this Policy, please contact the Chief Privacy Officer for **FacilicorpNB**, Kelly Steeves, at (506) 663-2500.