Reporting and Management of Information Privacy Breaches

1. Introduction

1.1. Purpose

The purpose of the Reporting and Management of Information Privacy and Confidentiality Breaches ("Policy") is to ensure suspected breaches of personal information, as defined in PHC Information Privacy and Confidentiality Policy, are reported and managed in an appropriate and timely manner.

1.2. Scope

This policy applies to all Staff and all Personal Information regardless of format or how it is stored or recorded.

2. Policy

2.1. Identifying a Privacy Breach

Staff must be able to identify a Privacy Breach.

A Privacy Breach is any loss, theft, unauthorized access to, collection, use, disclosure, or disposal of Personal Information, regardless of format. Any access to or disclosure of Personal Information outside the requirements of the job is also a privacy breach.

Examples of Privacy Breaches include, but are not limited to:

- Loss or theft of information stored on a laptop, personal computer, portable storage device, network device, electronic media, or recorded on paper or on other written or printed media;
- Staff intentionally accessing/viewing Personal Information other than that required to perform their job function; and
- Disclosure of Personal Information or disclosure beyond what others need to know to perform their job function.

2.2. Staff Response to a Privacy Breach

When Staff identify or suspect a Privacy Breach has occurred, they must:

a) Contain the Privacy Breach immediately;
b) Report the actual or suspected Privacy Breach to their Manager/Leader or Department Head and to the Information Access and Privacy Office (IAPO); and
c) Assist the IAPO in its investigation and follow-up as required.

Refer to Appendix A: Key Steps to Responding to Privacy Breaches, for more detailed steps when responding to a breach.

3. Responsibilities

3.1. Information Access & Privacy Office

- Maintain and administrate the policy
- coordinate investigations, identify risks, and document all privacy breaches;
- guide staff through the process of managing a privacy breach;
- manage privacy breaches in a manner that is consistent with the guidelines set out by the Information and Privacy Commissioner for British Columbia (OIPC) and other generally accepted practices;
- determine if affected individuals or organizations should be notified and how these individuals or organizations will be notified;
- notify the OIPC;
- notify other departments as appropriate e.g. Risk Management, Senior Leadership Team, Human Resources, Medical Affairs, Communications & Public Affairs;
- work to implement policies and practices that prevent privacy breaches; and
- develop and deliver privacy education to staff.

3.2. Leaders/Managers/Department Heads

- Ensure staff are aware of this policy and of their responsibilities for privacy breach reporting;
- ensure all privacy breaches are reported to the IAPO;
- cooperate and participate in the privacy breach investigation in a thorough and timely manner as requested; and
- undertake remedial and preventative follow-up action as recommended by the investigation**.**

3.3. Staff

- Immediately report an actual or suspected privacy breach;
- Will take immediate steps to contain a privacy breach;
- will cooperate with and assist in a privacy breach investigation in a thorough and timely manner; and
- will undertake remedial and preventative follow-up action as recommended by the investigation.

4. Compliance

Failure to comply with this policy may result in disciplinary action including, but not limited to, the termination of employment, loss of privileges as a student or volunteer role, prosecution and restitution for damages.

5. Supporting Documents

5.1 Related Policies

Cellular Phone and Blackberry Devices
Information Privacy and Confidentiality
Mobile Computing and Portable Storage Device Security
Safe Reporting
Information Security

6. Definitions

"FIPPA" means the *BC Freedom of Information and Protection of Privacy Act*, as amended from time to time.

"IAPO" means the PHC Information Access and Privacy Office

"OIPC" means the Office of the Information and Privacy Commissioner for B.C.

"Patients & Residents" mean all individuals receiving services from PHC. For ease of language, Clients and Assisted Living tenants are not specifically named but are implied in any reference to patient/resident.

"Personal Information" means recorded information about an identifiable individual other than contact information, such as a person's title, business telephone number, business address, email or fax number.

Examples of Personal Information include but are not limited to, name address, telephone number, personal healthcare number (PHN); race, national or ethnic origin, colour or religious beliefs or associations; age, sex sexual orientation, marital or family status; fingerprints, blood type or inheritable characteristics; health history, including any physical or mental disability; or educational, financial, criminal or employment history.

"Privacy Breach" occurs when there is an intentional or inadvertent unauthorized collection, use, disclosure, or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of the BC *Freedom of Information and Protection of Privacy Act (FIPPA)* and PHC's Confidentiality Policy (CPF0300). For the purpose of this policy, privacy breaches are managed the same whether suspected or confirmed.

"Staff" means all employees (including management and leadership), medical staff members (including physicians, midwives, dentists) and nurse practitioners, residents, fellows and trainees, health care professionals, students, volunteers, contractors, researchers and other service providers engaged by PHC.

7. References

B.C. Freedom of Information and Protection of Privacy Act (FIPPA)
Privacy breaches: tools and resources (OIPC)

8. Appendices

Appendix A: Key Steps in Responding to Privacy Breaches

Appendix A: Key Steps in Responding to Privacy Breaches

The following are the key steps to take if a Privacy Breach is suspected or confirmed:

1. Contain the Breach
2. Evaluate the Risk
3. Determine who needs to be Notified
4. Take actions to Prevent a recurrence

1. Contain the Breach

Take immediate, common-sense steps to limit the breach, including:

- Contain the breach (e.g. stop the unauthorized practice, recover the records, shut down the system that was breached, remove access to a system, or improve physical security);
- Activate the *Managing Privacy Breaches p*olicy;
    - Notify your Leader, Manager or Department Head
    - Notify the Information Access and Privacy Office (IAPO), who will provide assistance on breach containment
    - Notify Service Desk and/or Security (if applicable)
    - Notify police if theft or criminal activity is involved
- If the privacy incident occurs outside of normal business hours, report to the appropriate Clinical Coordinator or Leader on-call for the area. A follow-up report to your Leader/ Manager / Department Head and to the IAPO should take place not later than the next business day;
- Identify the personal information involved. Reproduce the information if possible.
- Do not destroy any evidence that may be valuable in determining the cause or will allow PHC to take appropriate corrective action.

2. Evaluate the Risks Associated with the Breach

To determine what other steps are immediately necessary, you must assess the risks. Factors to consider include:

<u>Personal Information involved</u>

- What data elements have been breached?
    - In general, the more sensitive the data, the higher the risk (e.g. health information, government-issued pieces of ID such as social insurance numbers (SIN), driver's license and health care numbers (PHN), financial account numbers such as credit or debit card numbers that could be used for identify theft). If possible, reproduce the data breached.

- What is the potential for the information to be used being used for fraudulent or otherwise harmful purposes (e.g. identity theft)?
- What is the context of the personal information involved? (e.g. name and address in a phone book would be less sensitive than name and address on a list of patients receiving counseling or a list of employees away on vacation)

Cause and extent of the breach

- What is the cause of the breach and the risk of ongoing or further exposure of the information?
- What is the extent of the unauthorized collection, use or disclosure and the risk of further access, use or disclosure, including in mass media or online?
- Was the information lost or stolen? If stolen, what is the likelihood that the information was the target of the theft?
- How many individuals are affected by the breach and what is their relationship to PHC (e.g. employees, public, contractors, patients/residents, service providers, other organizations)?
- Potential harm PHC may suffer from the breach (e.g. loss of trust, loss of assets, financial exposure);
- Is the information encrypted or otherwise not readily accessible?
- Has the information been recovered?
- What steps have you already taken to minimize the harm?
- Is this a systemic problem or an isolated incident?

Foreseeable harm arising from the breach

- Who is in receipt of the information? E.g. a stranger who accidentally receives personal information and voluntarily reports the mistake is less likely to misuse the information than an individual suspected of criminal activity.
- Is there any relationship between the unauthorized recipients and the data subject? E.g. a close relationship between the victim and the recipient may increase the likelihood of harm, such as an estranged spouse.
- What harm to individuals might result from the breach? Harm that may occur includes:
    - Security risk (e.g. physical safety)
    - Identify theft or fraud
    - Loss of business or employment opportunities
    - Hurt, humiliation, damage to reputation or relationships
- What harm could result to the public as a result of the breach, such as risk to public health or safety?

3. Notification

As deemed applicable to the specific privacy incident, notification may be required to one or more of the following:

- to the individuals whose information was involved in the incident
- to other organizations or groups affected by the incident (e.g. a Health Organization that PHC provides services to under Lower Mainland Consolidation)
- to the Office of the Information and Privacy Commissioner for B.C. (OIPC)

The PHC Information Access and Privacy Office will assist in determining if notification is required and the type of notification required. If required, direct notification is preferred – by phone, letter or in person. The IAPO will help in preparing notification material, such as notification letters and telephone scripts.

If notification is necessary it should occur as soon as possible following the breach. However, there may be circumstances where notification would be delayed, such as in cases where police have been notified and there is a criminal investigation going on.

4. Prevention

After immediate steps are taken to mitigate the risks associated with the breach, IAPO will work with the affected department to:

- Conduct a thorough risk-based investigation and analysis of the breach (may include a thorough security audit of both physical and technical security);
- Identify recommendations to prevent a recurrence of a similar incident;
- Review and update policies and procedures based on the lessons learned;
- Respond to any OIPC recommendations; and
- Provide education, if required.

Effective Date:	01-FEB-2008		
First Released:	01-FEB-2008		
Last Revised:	01-OCT-2022		
Last Reviewed:	01-OCT-2022		
Approved By:	PHC	PHSA	VCH
	Shaf Hussain	NA	NA
Owners:	PHC	PHSA	VCH
	Information Access & Privacy Office	NA	NA

Revision History: *(optional)*	**Version**	**Date**	**Description/ Key Changes**	**Revised By**
		01/OCT/2022	No material changes	Janet Scott