Category: Information Access and Privacy (IAP)	
Title: Managing Privacy and Confidentiality Breaches	**Reference Number:** IA_100
Approved by: Senior Executive Team	Last approved: April 27, 2015 Last reviewed: May 14, 2012

1. PURPOSE

The purpose of the Managing Privacy Breach Policy ("Policy") is to ensure the management of privacy and confidentiality breaches of Personal Information or 'Other Confidential Information' as defined in PHSA Privacy and Confidentiality Policy IA_020 in the custody or control of the PHSA or a Collaboration Organization. This Policy is intended to:

a. minimize and mitigate the potential risk of breaches;
b. enable a prompt, effective and orderly response to ensure breaches are contained and mitigated; and
c. ensure compliance with the requirements of the *BC Freedom on Information and Protection of Privacy Act (*FIPPA).

Capitalized terms in this Policy have the meaning assigned in the Definition section of this Policy.

2. SCOPE

The obligations in this Policy relating to Personal Information and Other Confidential Information (in any format including paper, electronic, film and verbal discourse) applies to Staff and Agents while in the course of working or conducting business for or on behalf of the PHSA or a Collaboration Organization, or when off-duty. The confidentiality obligations imposed by this Policy extends beyond the completion of the employment or business relationship.

3. BACKGROUND

PHSA is governed by FIPPA, the E-Health Act, and other legislation and standards of practice regarding protecting personal information. FIPPA in particular provides a framework for upholding privacy and confidentiality of Personal Information. There are privacy protection penalties for individuals and organizations who commit an unauthorized disclosure under FIPPA and / or the E-Health Act.

A violation of the Privacy and Confidentiality Policy (IA_020) may cause serious consequences for patients and Staff, as well as the PHSA as an organization.

4. POLICY STATEMENT

4.1 Containment

4.1.1 Upon discovering a suspected or confirmed privacy or confidentiality breach, PHSA Staff and Agents must take immediate steps to contain the breach, including:

- preventing any further loss, theft, or unauthorized practice/disclosures;
- recovering records; and
- securing the system or physical functional or operational area where the breach occurred (the "Area") to prevent further unauthorized practices/disclosures.

4.2 Reporting

4.2.1 Staff must immediately report suspected or confirmed breaches to their Manager or to the Information Access and Privacy (IAP) department. If a staff member is concerned about potential discrimination, retaliation or reprisal as a result of reporting a breach, they may report in accordance with the Safe Reporting Policy (AB 620).

4.2.2 The Manager must immediately notify the suspected or confirmed breach to IAP.

4.2.3 Managers must ensure that suspected or confirmed breaches that involve an identifiable patient(s) are entered into PHSA's Patient Safety Learning System (PSLS).

4.2.4 Staff must immediately report the theft or loss of electronic devices or electronic data held in PHSA systems to the PHSA Service Desk per the applicable IMITS policy Information Security policy. The servicedesk will then report to IAP. IAP will take appropriate follow-up actions where personalor confidential information may have been released.

4.3 Investigation, Assessment and Mitigation

4.3.1 Areas in which the Breach occurred are responsible for the investigation of the Breach. Each Area must assign a 'Lead' to investigate the alleged breach promptly unless the breach investigation is led by Information Management Information Technology Services (IMITS), Internal Audit (IA) or the Department Head/Professional Practice Leader when breaches relating to medical staff are investigated.

Note: When IA (but not IMITS) conducts the investigation, the investigation will be conducted in accordance with the applicable IA policy and the investigation under this Policy will cease. Department Heads/Professional Practice Leaders will conduct breach investigations in accordance with the applicable Medical Staff Bylaws and Rules.

4.3.2 The Investigative Lead will thoroughly investigate all matters related to a suspected or confirmed breach. The Investigative Lead will take action to mitigate risks resulting from the privacy breach in accordance with the Breach Management Guidelines.

4.3.3 IAP will act as a facilitator and advise the Area on the steps to be taken in the investigation of all reported suspected or confirmed breaches.

4.3.4 Depending on the nature of the suspected or confirmed breach other departments may participate in the investigation as outlined in the Roles and Accountabilities section of the Breach Management Guidelines.

4.3.5 Staff must fully cooperate in any investigation of a suspected or confirmed breach.

4.4 Notification

4.4.1 The impact of Breaches must be reviewed to determine if it is appropriate to notify individuals whose information has been affected by the breach. Considerations are documented in the Notification Tip sheet.

4.5 Failure to comply

4.5.1 Failure by Staff and Agents to comply with this Policy may lead to disciplinary action up to and including termination or suspension of employment, the loss of computer privileges, loss of privileges associated with a student placement or volunteer role, suspension / restriction / modification / termination of medical staff privileges or cancellation of contractual arrangements.

4.6 Material Risks

4.6.1 Where there is material risk to individuals, PHSA or other organizations resulting from any Breach, IAP shall promptly report the breach to Risk Management.

5.0 EXCEPTIONS

There are no exceptions.

6.0 RELATED POLICIES AND RESOURCES

Listed below are related PHSA policies:

- Privacy and Confidentiality
- Fraud, Theft and Corruption Policy
- Safe Reporting Policy
- Information Security policy

Listed below are related PHSA resources:

- PHSA Privacy and Confidentiality Breach Management Guidelines and related tip sheets:
    - Levels of Privacy Breaches
    - Notification tip sheet
    - Investigative Questions tip sheet

- Breach reporting form
- Privacy and Security 101

7.0 DEFINITIONS

Refer to Privacy and Confidentiality (IA_020) for definitions of **Clients**, **Staff**, **Agents**, **Collaboration Organization**, and **Other Confidential Information**.

Area means a PHSA operational or functional area;

- **Breaches** are the loss, theft, intentional or inadvertent unauthorized collection, use, disclosure, storage or disposal of Personal Information or Other Confidential Information inthe custody or control of the PHSA or Collaboration Organization. Such activity is "unauthorized" if it occurs in contravention of Part 3 of the FIPPA or PHSA's Privacy and Confidentiality

IAP means the PHSA Information Access and Privacy office;

Investigative Lead means the individual assigned by the Area to lead the investigation;

Manager means the person overseeing the activities of Staff in an Area and Management means one or more Manager;

Personal Information is recorded information about an identifiable individual other than contact information. For examples of Personal Information refer to the IAP Pod Pages.

8.0 REFERENCES

Office of the Information and Privacy Commissioner of BC Resources – Privacy Breach Management Policy Template

Freedom of Information and Protection of Privacy Act

E-Health (Personal Health Information Access and Protection of Privacy) Act