Reporting and Management of Information Privacy Breaches

1. Introduction

Description
Privacy Breaches occur when Personal Information has been lost, stolen or disclosed without authorization, whether accidentally or intentionally. The purpose of this policy is to ensure proper management of Privacy Breaches.

Scope
This policy applies to all Staff, including physicians, and all Personal Information whether in electronic, paper or other form.

2. Policy

2.1. Identifying a Privacy Breach

A Privacy Breach is a loss, theft or unauthorized access (paper or electronic) of Personal Information. Any disclosure of Personal Information outside the requirements of the job is also a Privacy Breach.

Some examples of Privacy Breaches include:

- Staff intentionally viewing Personal Information other than that required to perform their job function;
- 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; and
- Unauthorized 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

Staff must follow three steps when responding to a Privacy Breach. If there is an actual or suspected Privacy Breach, Staff will:

1. Contain the Privacy Breach immediately. See 2.3, Containing the Privacy Breach.
2. Report the actual or suspected Privacy Breach to their Manager/Supervisor or Department Head and to the VCH Information Privacy Office (IPO). Staff must also work with their Manager to initiate and complete a Patient Safety Event Report. See 2.4, Reporting actual or suspected Privacy Breach.
3. Assist the IPO in its investigation and follow-up, as required. See 2.5. Investigation and Notification of Privacy Breaches.

2.3. Containing the Privacy Breach

Staff will act immediately to contain the Privacy Breach. This may include actions such as: stopping the unauthorized practice; recovering records; securing a system; correcting or enhancing physical security; and/or contacting Integrated Protection Services, the Police, or Service Desk.

The IPO can provide more information and assistance on containing a Privacy Breach.

2.4. Reporting Actual or Suspected Privacy Breach

2.4.1. Reporting Theft or Loss of a Device (including Portable Storage Device)

Staff will immediately report a lost or stolen VCH-issued device to the Service Desk as per the Cellular Phone and Blackberry Devices policy and the Mobile Computing and Portable Storage Device policy.

Staff will report a lost or stolen personal portable storage device containing Personal Information to their Supervisor/Manager or Department Head and to the IPO. Staff must also work with their Manager to initiate and Report a Safety Event.

2.4.2. Reporting Theft or Loss of Information

Staff will immediately report an actual or suspected Privacy Breach resulting from theft or loss of information to their Supervisor/Manager or Department Head and to the IPO. Staff must also work with their Manager to initiate and Report a Safety Event.

2.4.3. Whistleblower Protection

In accordance with the Information Privacy & Confidentiality and Whistleblower policies, Staff members are protected against retaliation and disciplinary measures when reporting actual or suspected privacy breaches, so long as they are acting in good faith and on the basis of reasonable belief.

2.5. Investigation and Notification of Privacy Breaches

The IPO will promptly and thoroughly investigate the actual or suspected Privacy Breach and will take appropriate action to contain and mitigate risk arising from a Privacy Breach.

Staff will assist the IPO in its investigation. Upon request, Staff will provide supporting documentation, assist in notifying affected Clients (if required) and assist in determining and implementing safeguards to prevent further incidents.

The IPO will determine whether notification of the Privacy Breach must be made to the Clients affected and/or to the Office of the Information and Privacy Commissioner for British Columbia (OIPC).
The IPO will consider the following factors when deciding to notify Clients or the OIPC:

- The sensitivity of the information;
- What harm might arise from the Privacy Breach, including whether it could be used for identity theft or other harmful purposes;
- Number of people affected and their relationship to VCH;
- Whether the information could easily be exploited for reasons it was not intended for;
- The extent of any residual risks associated with the incident once it has been contained; and
- Whether notification may cause harm to the individual affected by the Privacy Breach.

### 2.6. Responsibilities

#### 2.6.1. Staff

- Staff will immediately report an actual or suspected Privacy Breach as described above.
- Staff will cooperate with and assist in an investigation of a Privacy Breach in a thorough and timely manner.
- Staff will take immediate steps to contain a Privacy Breach, for example, by seeking return of records or enhancing physical (e.g. changing locks) or technological (e.g. changing password, secure network folder) security measures.

#### 2.6.2. Management

- Management will assist their Staff and cooperate with the IPO in an investigation of a Privacy Breach in a thorough and timely manner.

#### 2.6.3. Information Privacy Office

The IPO will:

- Investigate, coordinate, and document all Privacy Breaches.
- Guide Staff through the process of managing a Privacy Breach.
- Take steps to contain a Privacy Breach, for example, seeking return of records or enhancing physical or technological security measures to mitigate risks associated with the Privacy Breach. See Guidelines on Handling Privacy Breaches.
• Manage Privacy Breaches in a manner that is consistent with the guidelines set out by the OIPC, Ministry of Health and other generally accepted practices.

• Decide whether the affected individuals or organizations should be notified of a Privacy Breach and how these individuals or organizations (including the OIPC) will be notified.

• Where there is a risk to individuals, VCH or other organizations resulting from a Privacy Breach, promptly report the Privacy Breach to VCH Risk Management, Communications and Public Affairs, and/or to Legal Services.

• Update, implement and monitor this policy.

• Work to implement policies and practices that prevent Privacy Breaches.

• Develop and provide privacy education to Staff and promote awareness of this policy and related privacy policies and guidelines.

2.7. Compliance

Failure by Staff to comply with this policy may result in disciplinary action including, but not limited to, the loss of computing privileges, termination of employment, loss of privileges as a student placement or volunteer role, and legal action by VCH and/or others.

3. References

Tools, Forms and Guidelines

• British Columbia Freedom of Information and Protection of Privacy Act
• Guidelines on Handling Privacy Breaches
• SLS – Report a Safety Event
• VCH Information Privacy Office Intranet

Related Policies

• Cellular Phone and Blackberry Devices
• Information or Information Storage Device, Reporting Theft or Loss of
• Information Privacy and Confidentiality
• Information Security
• Mobile Computing and Portable Storage Device Security
• Whistleblower
Keywords
clients, FIPPA, guidelines, OIPC, personal information, privacy, privacy breach, privacy breach reporting, reporting, staff

Definitions
"Clients" means all people receiving services from VCH and includes patients and residents.

"Personal Information" means any information about an identifiable individual but does not include business contact information (e.g. individual’s title, business telephone number, business address, business email or facsimile number).

“Privacy Breach” or “Breach” occurs when there is unauthorized access to or collection, use, disclosure or disposal of Personal Information. Such activity is “unauthorized” if it occurs in contravention of Part 3 of the *Freedom of Information and Protection of Privacy Act*.¹

“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 and other service providers engaged by VCH.

Questions
Contact: Information Privacy Office at privacy@vch.ca or (604) 875-5568