See also: 1.5.4PR Breach Risk Assessment and Ranking Procedure

1.0 General Administrative

1.5 Privacy and Confidentiality

1.5.4 Privacy and Related Information Security Breaches: Reporting, Investigation and Management

1.0 Purpose

This policy identifies the requirements, roles and responsibilities of staff (includes management and physicians as per attached definition) when there is the potential for or an actual breach of the information privacy or security of Sensitive Information.

2.0 Policy

VIHA staff must report, investigate and manage all potential and actual violations or breaches of the Information privacy or security of Sensitive Information in a timely, systematic, and effective manner in accordance with the *Freedom of Information and Protection of Privacy Act* (FIPPA **http://www.qp.gov.bc.ca/statreg/stat/F/96165_00.htm**)

When any staff member becomes aware of a potential or actual violation or breach of Sensitive Information, they will follow the CAN DO protocol:

- **CONTAIN** incident immediately to limit its impact;
- **ASSESS** its associated impact on the person(s) whose Sensitive Information was potentially or actually breached;
- **NOTIFY** their direct Manager/Supervisor or if after-hours, the Administrator On-Call immediately. If unable to make contact within 1 hour of discovery of incident, notify the Information Access and Privacy Office (IAP) at 1-877-748-2290 or 250-519-1870;
- **DOCUMENT** the facts as requested and;
- **OFFER** to assist in the investigation and prevention of subsequent incidents.

3.0 Additional Roles and Responsibilities

Additional responsibility for reporting, investigation and follow-up is dependent on a person's organizational role and the nature of the incident.

3.1 Staff (Non-supervisory)

In implementing the CAN DO protocol, staff will also:

1. **Contain** incident to limit its impact by acting to stop further spread of the compromised Sensitive Information. For example, by locking rooms, locking computers, retrieving and securing papers, mobile devices or other forms of

information not properly stored or secured or by requesting individuals discussing Sensitive Information in public places to stop.

2. Assess its associated impact by taking note of the nature, circumstances and time, what Sensitive Information was compromised and how that occurred, what role the physical environment had in the incident and all involved individuals to identify and minimize any immediate risks of harm to the patient, other involved persons, staff or the organization.

3. Notify their responsible Supervisor/Manager, Administrator on Call or the IAP Office (as appropriate) of the incident, the immediate containment steps taken and details of the assessment of its impact.

Staff will, if requested by their Supervisor or a representative of the IAP Office; document the facts and actions taken by completing the *Breach Assessment Reporting and Incident Management Tool*..\Web Forms\breach_assessment_reporting_incident_management_tool.doc

3.2 The Role of the Supervisor / Manager or Administrator On-Call

Upon being informed of a potential or actual privacy breach, the Supervisor/Manager, or Administrator On-Call will:

1. Assist, as necessary, their staff member with completing the CAN DO protocol;
2. Assess and assign an initial risk ranking for the incident (refer to 1.5.4PR Breach risk assessment and ranking for direction);
3. Immediately notify the IAP Office @ 1-877-748-2290 or 250-519-1870 if not already notified;
4. For incidents assessed as LOW or MODERATE risk, notify the program area functional officer using normal channels of communication. If their Director/Medical Director or Executive On-Call is unavailable, notify the next level Functional Officer. If Incident ranked as HIGH or EXTREME, ensure notification occurs immediately to allow for compliance with policy 1.2.1 *Immediate Notification of an Emerging Issue/Untoward Incident.*
5. Contact their Human Resources consultant if an employee is suspected to be involved in the breach and;
6. Document or assign delegate to document their containment actions, initial assessment and risk ranking on the Breach Assessment Reporting and Incident Management Tool ..\Web Forms\breach_assessment_reporting_incident_management_tool.doc and submit electronically to the confidential email address Privacy@VIHA.ca or fax to (250)-370-8971.
7. Participate in the breach investigation, further risk assessment, notification, management and prevention of subsequent incidents.

The investigation and follow-up will be supported by the IAP Office and an Integrated Breach Response Team (IBRT) consisting of resources appropriate to the nature and risk level of the incident, including IM/IT Security staff, Human Resource Consultants and other relevant key stakeholders.

3.3 The Role of the Director, Executive Director and/or Executive Medical Director or Executive on Call

Upon being informed of a potential or actual privacy breach the Director, Executive Director and/or Executive Medical Director or Executive on Call will:

1. Notify Senior Executive of breaches with an initial risk ranking of HIGH or EXTREME using the Emerging Incident Form in accordance with policy *1.2.1 Immediate Notification of an Emerging issue/Untoward Incident. F*or breaches assessed as LOW or MODERATE risk, notify the program area functional officer using normal channels of communication;
2. Participate as required in the investigation, management of the incident and prevention of further incidents.

3.4 The Role of the Information Access & Privacy (IAP) Office, IM/IT Security Office and Human Resources Consulting (HRC)

The IAP, IM/IT Security and HRC offices have a responsibility, in collaboration with the involved area(s) and stakeholders, to:

1. Investigate, track and trend all information privacy and related information security incidents and their associated privacy risks;
2. Assess, validate and modify as necessary, the initial risk ranking assigned to the incident by the Supervisor/Manager or Administrator On-Call; and confirm that organizational notification relevant to the incident has been initiated as per s. 3.3.
3. Assign an IAP lead and assemble the appropriate IBRT members, relative to the incident's nature and risk, to coordinate the investigation and management of the incident and take action to fully contain, assess and mitigate risk arising from the incident;
4. Assign a final risk ranking to the incident based on the findings of the investigation;
5. Update relevant stakeholders, regarding progress and outcome of incident management.
6. Coordinate the timing, nature of and responsibility for additional notification** of individuals and/or organizations affected by the breach, including the BC Office of the Information and Privacy Commissioner, as appropriate to the issue.
7. Conduct a Root Cause Analysis (may include a security audit of both physical and technical security) and a risk-based analysis of long-term safeguards;
8. Review and update policies and practices and provide refresher training on privacy and security obligations and;
9. Submit a report to relevant stakeholders and the VIHA Board of Directors on an annual basis or as otherwise requested.

**Notification: Relevant factors that will impact	
1. **Timing and nature of notification include:**	• The kind of information compromised and its sensitivity.
	• Ease of exploitation for fraudulent or otherwise harmful reasons.
	• Potential or actual harm to the individual and organization arising from the incident.
	• Number of people affected and their relationship to VIHA.
	• Cause of the incident.
	• Degree to which information was recovered.
	• Degree of residual risk associated with the incident once it has been contained.
2. **Additional persons who may require notification include: if there is suspected or actual:**	• Negative impact to the health record– Director, Health Records.
	• Employee misconduct – Union representative.
	• Theft, criminal activity or physical security breach – Manager, Protection Services.
	• Professional misconduct of a regulated health professional – Professional Practice Office or Medical Affairs Office if MD involvement.
	• Confirmed misconduct or theft by a member of a Professional Regulatory Body - Appropriate Regulatory Body (e.g. CRNBC).

Notification will be immediate when it is necessary to avoid or mitigate harm to the individual(s) whose personal information has been compromised or when required by law.

4.0 Applies to

This policy applies to all staff and to all Sensitive information for which VIHA has custody or control responsibilities, whether that information is in paper, electronic or other format. Personal information may be about clients or staff.

It does not apply to Information security incidents that do NOT contain Sensitive Information (e.g. theft of physical asset containing no Sensitive Information).
It does not apply to anonymous, aggregate or appropriately de-identified data that cannot be linked to an identifiable individual, or to business contact information**.**

5.0 Definitions

Business Confidential Information is business information as defined in Confidentiality policy 1.5.2 that requires security protections to prevent unauthorized disclosure. This may include intellectual property or specific details related to security controls and operational procedures that could cause hardship to the business or to others if obtained for malicious purposes.

Business Contact Information is information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual.

Clients are people receiving services from VIHA including patients and residents.

Information Security Breach is an incident or event that negatively impacts the confidentiality, integrity, or availability of VIHA Sensitive information or information systems. An individual obtaining unauthorized access to VIHA information systems is an example of a security breach.

Integrated Breach Response Team (IBRT) is a team of key representatives from involved program areas and VIHA leadership who are organized to collectively share their expertise and skills in managing, mitigating, resolving and undertaking a post-incident quality improvement review of breaches with a risk rating of High or Extreme. The IBRT will consist of members from the following programs: Privacy & Information Security Offices, Risk Management, Internal Audit, Involved Business Area Leadership, IM/IT Leadership, Health Records, QPS Leadership, and Human Resources Consulting Service, who will be engaged as appropriate to the specific nature and risk level of the incident.

Personal Information is identifiable information about an individual (including but not limited to patients, clients, residents, volunteers, students, staff, physicians or members of the public), but it does not mean business contact information. Personal information includes things such as a person's name, social insurance number, account number, health care number, employment history or medical information. References to "personal information" within this policy apply to any documents or records (whether in hard copy or electronic form) on which personal information is recorded and all verbal comments or conversations in which personal information is mentioned or discussed.

Potential Privacy or Information Security Breach is the identification of possible unauthorized activities as set out above which, if the risk is not mitigated, may result in an actual breach. This may include careless information management practices such as unsafe storage or disposal of personal information.

Privacy Breach is the unauthorized access to, collection, use, disclosure, retention, disposal or protection of personal information in the custody or under the control of VIHA. Such activity is "unauthorized" when it occurs in contravention of Part 3 of the FIPPA or other relevant legislation. A misdirected email or fax containing personal information is an example of a privacy breach.

Privacy or Information Security Violation is the occurrence of a particular incident that disregards information privacy and security policies, but does not necessarily result in a breach. Installation of unauthorized software on a VIHA device containing Sensitive Information is a security violation. Using authorized means to access to one's own personal information for unauthorized (non work-related) purposes is a good example of a privacy violation.

Sensitive Information for the purposes of this policy is both the definitions of "Business Confidential" and "Personal Information."

Staff are all officers, directors, employees, physicians, health care professionals, students and/or volunteers engaged by VIHA and contractors and their employees as set out in FIPPA.

6.0 Related VIHA Policies & Procedures

- 1.2.1 Immediate Notification of an Emerging issue/Untoward Incident
- 1.5.1 Confidential Information – Privacy Rights of Personal Information VIHA Policy
- 1.5.2 Confidential Information – Confidential Information – Third Party, VIHA Business and Other Non-Personal Information Policy
- 1.5.3 Release of Patient Information to Law Enforcement Personnel in Urgent or Emergency Situations (in the Absence of Patient Consent, Court Order or Search Warrant)
- 1.5.4PR Breach Risk Assessment and Ranking Procedure
- 1.6.1 Enterprise Risk Management
- 1.6.1PR Enterprise Risk Management Procedure
- 5.6.4 Corrective Discipline
- 16.4.2.1 Security of Electronic Information
- 16.4.2.2 Security of Health Records
- 16.4.2.3 Acceptable Use of Assets and Resources
- 16.4.2.4 Remote Access
- 16.4.2.5 Mobile Computing

References

BC Office of the Information and Privacy Commissioner “Key Steps in Responding to Privacy Breaches” http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches(June2008).pdf

Freedom of Information & Protection of Privacy Act. R.S.B.C. 1996, c. 165, http://www.qp.gov.bc.ca/statreg/stat/F/96165_00.htm

Interior Health Authority AR0450 Policy – Managing Privacy & Security Breaches/Violations (November 2007)

Ministry of Health (DRAFT) e-Health Privacy Breach Response and Reporting Policy (June 2007)

Ministry of Health Knowledge Management and Technology Division (DRAFT) Policy - Privacy Breach Response and Reporting (2006)

University of Florida Privacy of Health Information Operational Guidelines: Reporting, Investigating, and Responding to Privacy Violations Policy (Rev. November 2004)

Vancouver Coastal Health Authority Policy - Management of Information Privacy Incident (June 2006)