Administrative Policy Manual

Code: AR Information Privacy and Security

AR0450 – MANAGING PRIVACY & SECURITY BREACHES / VIOLATIONS

Interior Health would like to recognize and acknowledge the traditional, ancestral, and unceded territories of the Dãkelh Dené, Ktunaxa, Nlaka'pamux, Secwépemc, St'át'imc, Syilx, and Tŝilhqot'in Nations, where we live, learn, collaborate and work together.

Interior Health recognizes that diversity in the workplace shapes values, attitudes, expectations, perception of self and others and in turn impacts behaviors in the workplace. The dimensions of a diverse workplace includes the protected characteristics under the human rights code of: race, color, ancestry, place of origin, political belief, religion, marital status, family status, physical disability, mental disability, sex, sexual orientation, gender identity or expression, age, criminal or summary conviction unrelated to employment.

1.0 PURPOSE

The purpose of this policy is to promote a standardized process for addressing Potential or Confirmed Information Privacy and Information Security Breaches and Violations to enable Interior Health (IH) to respond effectively and consistently to Information Privacy and Information Security Breaches.

2.0 DEFINITIONS

TERM	DEFINITION
Clients	*Patients and persons in care in IH facilities and programs.*
Confidential Information	*Whether oral, written, electronic or film, includes the following:* *a) Personal Information (see definition below).* *b) Business information collected or created by IH that exists regardless of form and includes, but is not limited to:* • *Information provided to IH by an external vendor or service provider which, if disclosed, would harm the business interests of the third party;* • *Information prepared as part of pending or ongoing litigation, law enforcement investigation, quality assurance review, Workers Compensation Board or Ombudsman investigation;* • *Information related to credentialing, discipline, privilege, quality assurance reviews and external review of quality of care;*

	• *In-camera deliberations of IH where such topics as budget strategies, personnel, labor relations, land acquisitions or litigation may be discussed;* • *Unpublished statistical information and internal correspondence related to organizational initiatives; and* • *Information supplied in confidence to a mediator or arbitrator to resolve or investigate a labor relations dispute.* *c) All information that, if disclosed without authorization, could be prejudicial to the interests of IH and associated individuals or agencies; and Organizational business information that would harm IH's financial interests and/or information that relates to the management of IH that has not yet been implemented or made public; such as information that identifies the security architecture and infrastructure of the organizations' information systems.*
Confirmed Breach or Breach	*Unauthorized access, collection, use, disclosure, storage, or disposal of Personal Information in the custody of or under the control of IH which contravenes the Freedom of Information and Protection of Privacy Act (FIPPA) or other legislation has occurred / been confirmed.*
Confirmed Violation or Violation	*An incident which contravenes IH Information Privacy and/or Information Security policies. For purposes of this policy, a Violation differs from a Breach in that a Violation does not result in a Breach of FIPPA; only a Breach of IH policies.*
Information Privacy	*An aspect of data protection for protecting Personal Information from unauthorized access, collection, use, disclosure, storage or disposal.*
Information Security	*Protecting information and information systems from unauthorized access, collection, use, disclosure, storage, disruption, modification, or disposal in order to provide confidentiality, integrity, and availability (CIA).*
Personal Information	*Includes any information which may be associated with or identifies an individual except business contact information. Personally identifiable information includes things such as a person's name, social insurance number, account number, health care number, employment history or medical information.*

	Does not include business contact information, such as a person's title, business telephone number, business address, email or facsimile number. *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 Breach/Violation	*The possibility of unauthorized access, collection, use, disclosure, storage, disposal of Personal Information, or contravention of IH policy is suspected or has been identified. This needs to be investigated to verify if there is or is not a Confirmed Breach*
Serious Privacy Breach Incident (Serious Breach)	*A Serious Breach is defined as an incident that meets the criteria outlined in the Information Privacy Incident Response Procedure section based on assessment of harm, containment of the Breach, extent of the Breach, sensitivity of the information and volume of affected individuals.* *Serious Breaches may be cybersecurity related (e.g. hacked system) or non-cybersecurity related (e.g. lost/stolen physical records).* *The Manager, Information Privacy and Freedom of Information is responsible for determining when a Breach meets this criteria.*
Users	*Includes all employees, medical staff, independent contractors, students, volunteers, and any other persons acting on behalf of IH.*

3.0 POLICY

3.1 Users are responsible for keeping Personal Information secure.

Note that this policy relates to Information Privacy and Information Security. Refer to Corporate Protection Services for any policies related to physical security.

3.2 All Potential and Confirmed Breaches and Violations must be reported to the IH Information Privacy and Information Security offices in accordance with the procedures of this policy (section 4.0).

3.3 Failure to comply with acceptable use standards will result in consequences that may lead to termination of access, employment and/or contract, withdrawal of privileges in accordance with Medical Staff Bylaws, and/or professional sanctions.

4.0 PROCEDURES

4.1 User Responsibilities (independent contractors see section 4.2)

4.1.1 Reporting Breaches and Violations

Upon learning of a Breach or Violation (or if unsure whether a situation constitutes a Breach or Violation), Users are required to immediately report the incident to

- Information Privacy directly **during regular office hours** at 1-855-980-5020 or IHPrivacy@interiorhealth.ca; or
- IMIT Service Desk **outside of regular office hours** at 1-855-242-1300. Details of the Breach/Violation including date/time of discovery, location and containment steps should be available; and
- your immediate Leader/Manager.

4.1.2 Containment

Upon recognizing a Potential or Confirmed Breach/Violation Users must take immediate steps to contain the Breach. This includes, but is not limited to recovering misdirected documents, searching the immediate vicinity for lost records, instructing an unauthorized recipient of a misdirected email to double delete the email and attachments and to provide written confirmation of the deletion, etc. Double delete refers to deleting the email from the main folder (inbox and/or sent folder, followed by the deleted items/trash/bin folder).

4.1.3 Cooperation during Investigation

Users must assist Information Privacy and/or Information Security in the course of responding to a Potential or Confirmed Breach/Violation.

4.2 Independent contractors (includes service providers and vendors) Responsibilities

Independent contractors are obligated under FIPPA and as a service provider to IH to comply with FIPPA and this policy.

4.2.1 Reporting Breaches and Violations

Independent contractors must provide immediate written notice of any Potential or Confirmed Breach/Violation. Independent contractors are required to immediately report the incident to the contact listed in the Service Agreement/Contract, the Manager/Director of the program area they are providing services to, IH Contracted Services, and/or Information Privacy.

4.2.2 Containment

Independent contractors must take immediate steps upon recognizing a Potential or Confirmed Breach/Violation to contain the Breach/Violation. This includes, but is not limited to recovering misdirected documents, searching the immediate vicinity for lost records, instructing an unauthorized recipient of a misdirected email to double delete the email and attachments and to provide written confirmation of the deletion, etc.

The external organization and/or Manager must follow up with their employee to ensure that immediate steps have been taken to contain and to minimize risks from the Breach/Violation.

4.2.3 Cooperation during investigation

All independent contractors and where applicable, the external organization, is expected to assist Information Privacy and/or Information Security in the course of responding to a Potential or Confirmed Breach/Violation.

4.3 Manager Responsibilities

4.3.1 Reporting Breaches and Violations

Upon being advised by User(s) of a Breach or Violation (or if unsure if a reported situation constitutes a Breach or Violation), department managers must confirm that the incident has been reported to Information Privacy and/or Information Security as per Section 4.1.1 of this policy. In the event that no notification has occurred the department manager will immediately report required details as per 4.1.1 to Information Privacy and/or Information Security.

Additionally, Managers must

- report incidents involving employees to Employee Relations;
- report incidents that may cause harm to the reputation of IH, such as social media posts by Users or patients, to IH Media; and
- report incidents to your respective leadership.

4.3.2 Containment

Immediately upon notification of a Potential or Confirmed Breach/Violation, ensure that immediate steps have been taken to contain and to minimize risks from the Breach/Violation. This includes, but is not limited to recovering misdirected documents, searching the immediate vicinity for lost records, instructing an unauthorized recipient of a misdirected email to double delete the email and attachments and to provide written confirmation of the deletion, etc.

Consult with Information Privacy and Information Security to preserve evidence needed for the investigation

4.3.3 Cooperation during Investigation

Managers must assist Information Privacy and/or Information Security in the course of responding to a Potential or Confirmed Breach/Violation.

4.3.4 Notifications

- When department managers receive a letter/script from Information Privacy, they will notify affected individual(s) as soon as possible. This is a FIPPA requirement. Department managers will use the delivery modality recommended by Information Privacy.
- Managers will report to Information Privacy as soon as reasonably possible:
  - The date/time the notification was completed.
  - All responses or feedback received from affected individuals, in summary format (e.g. individual upset, individual is understanding, etc.).

4.4 Information Privacy Responsibilities

4.4.1 Upon receipt of a Potential or Confirmed privacy Breach/Violation, Information Privacy will conduct an investigation. In the case of a Serious Breach/Violation, Information Privacy will report to the BC Office of the Information & Privacy Commissioner (OIPC) to comply with legislative requirements of FIPPA and liaise with Users regarding such reports and resulting recommendations from the OIPC.

4.4.2 Information Privacy will base the assessment for risk of significant harm on the Personal Information involved in the Breach and in accordance with FIPPA section 36.3. If notification to affected individuals is required, Information Privacy will draft the letter/script and will notify the OIPC. Note that notification to the OIPC may still occur regardless of whether notification to affected individuals is completed.

4.4.3 In the case of a Serious Breach, the Manager, Information Privacy and Freedom of Information, or delegate will activate the IH Information Privacy Incident Response Procedure (IPIRP).

4.4.4 Detailed Information Privacy Incident Response Procedure activation criteria is found within the Incident Response Procedure document.

4.5 Information Security Responsibilities

4.5.1 Upon receipt of a Potential or Confirmed security Breach/Violation, Information Security will conduct an investigation. In the case of a serious Breach/Violation, Information Security may work with Information Privacy to identify next steps. For serious security Breaches, Information Security may need to activate the IH Cybersecurity Incident Response Plan.

4.5.2 Detailed activation criteria is found within the Cybersecurity Incident Response Plan document.

4.6 Examples of Information Privacy or Information Security Breaches & Violations – See Appendix A

5.0 REFERENCES

1. AR0400: Privacy & Management of Confidential Information
2. Medical Staff Bylaws
3. Freedom of Information & Protection of Privacy Act (FIPPA or FOIPPA)
4. OIPC Privacy Breach Checklist

AR0450 – MANAGING PRIVACY & SECURITY BREACHES / VIOLATIONS

APPENDIX A - Examples of Privacy or Security Breaches & Violations

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

1. Accessing the health record of any patient you are not currently providing direct care for in any clinical system, including family members, friends, former patients or co-workers;

2. Accessing your own health record in any clinical system while using the credentials provided to you for the purposes of employment;

3. Sharing or providing your User ID and password to another individual for your own or others' convenience; you are accountable for all activity that occurs using your credentials and will be held responsible for accesses which are found in Breach;

4. Leaving your computer or any device unattended while signed in without locking it or logging off;

5. Leaving documents containing Client or Confidential Information in an area accessible or viewable by the public, or other co-workers who are not obliged to see the information;

6. Disposing of Client or Confidential Information in a regular refuse container and not a secure shredding container;

7. A misdirected email, print job or fax containing Client or Confidential Information;

8. Sending an email that contains Client or Confidential Information that is not encrypted;

9. Asking a co-worker for Client or Confidential Information you do not need to do your job;

10. Not taking reasonable care to secure assets at work and whilst in transit; e.g. leaving a mobile computing device, such as a laptop or smartphone unsecured in a public area, office, or in obvious sight in a vehicle, which elevates the risk of theft. The theft or loss of a laptop may be the result of failing to comply with the laptop guidelines, thus resulting in a security Violation;

11. Downloading and installing unauthorized software, including files such as music or video, screen savers, voice over internet software;

12. Using social media such as Facebook, Twitter, Instagram, Slack, and Reddit to post information that could damage the reputation of IH, or cause a Breach in Client privacy;

13. Lending your keys to someone else to permit them to access secure cabinets, offices or storage areas where patient or Confidential Information is stored;

14. Failing to report a Breach or Violation. All calls / emails to IH's Information Privacy or Information Security offices are kept in strict confidence.