Alberta Health Services

POLICY

TITLE
INFORMATION SECURITY AND PRIVACY SAFEGUARDS

SCOPE
Provincial

DOCUMENT #
1143

APPROVAL AUTHORITY
Corporate Services Executive Committee

INITIAL EFFECTIVE DATE
January 10, 2012

SPONSOR
Legal & Privacy / Information Technology

REVISION EFFECTIVE DATE
October 16, 2019

PARENT DOCUMENT TITLE, TYPE AND NUMBER
Not applicable

SCHEDULED REVIEW DATE
October 16, 2022

NOTE: The first appearance of terms in bold in the body of this document (except titles) are defined terms – please refer to the Definitions section.

If you have any questions or comments regarding the information in this document, please contact the Policy & Forms Department at policy@ahs.ca. The Policy & Forms website is the official source of current approved policies, procedures, directives, standards, protocols and guidelines.

OBJECTIVES

- To outline Alberta Health Services' (AHS) safeguards and standards to protect the **security**, privacy, and confidentiality of information in the custody and control of AHS.
- To support the expected InfoCare behaviours of **AHS people** when handling information and to meet AHS' legal obligations as a public body holding **personal information** and as a custodian of **health information**.

PRINCIPLES

AHS has a duty to protect the security, privacy, and confidentiality of information in its custody and control. Information security and privacy safeguards implemented by AHS help to ensure the integrity and accuracy of AHS' information are maintained. These safeguards ensure AHS is able to assess and manage risks associated with the collection, use, and disclosure of information in its custody and control.

All AHS people shall conduct themselves in accordance with the expected InfoCare behaviours and to access AHS resources and training as provided to educate themselves on the protection of health, personal, and **business information** as applicable to their roles and responsibilities.

APPLICABILITY

Compliance with this document is required by all Alberta Health Services employees, members of the medical and midwifery staffs, Students, Volunteers, and other persons acting on behalf of Alberta Health Services (including contracted service providers as necessary).

ELEMENTS

1. Training and Awareness

1.1 The Information & Privacy Office and Information Risk Management shall provide education and training on information security and privacy principles (information security and privacy training) to ensure all AHS people have sufficient awareness to protect the security, privacy, and confidentiality of AHS information.

1.2 Completion of AHS' information security and privacy training is mandatory. All AHS people with access to AHS restricted, confidential, or protected information (see the *Information Classification* Policy) shall complete the provided information security and privacy training on commencement of their duties with AHS, and at least once every three years thereafter.

1.3 AHS people who do not complete the information security and privacy training as required, and whose roles require them to access information, shall not be granted access or shall have their access to information suspended until the training has been completed.

1.4 Upon appointment, AHS people shall sign and, where required, update according to their role, the AHS confidentiality and user agreement.

2. Auditing

2.1 AHS shall implement auditing processes to ensure that access to information in its custody and control complies with applicable legislation and AHS policies and procedures.

2.2 Internal Audit may conduct audits of applicable AHS information security and privacy policies and procedures. Recommendations from each audit shall be considered and, where appropriate, addressed by the AHS Information & Privacy Department and Information Risk Management in collaboration with key stakeholders (e.g., Protective Services and **repository owners**).

2.3 Repository owners shall undertake annual assessments to determine compliance with Privacy Impact Assessments and related AHS policies and procedures. Repository owners shall:

a) submit the findings of the assessments to the Information & Privacy Department and Information Risk Management for review; and

b) address recommendations arising from the review.

3. Reporting and Responding to Breaches

3.1 AHS people shall, upon discovery of a **breach**, take immediate action to contain and recover any information involved within a breach.

3.2 AHS people shall immediately report the breach to the Information & Privacy Department or Information Risk Management, as appropriate. When responding to a breach, AHS people shall:

a) cooperate with the assigned Information & Privacy or Information Risk Management investigator;

b) notify affected individuals about the breach upon the recommendation of the assigned investigator;

c) ensure recommendations made by the investigator are implemented within their program area;

d) document any outstanding security and privacy risks; and

e) ensure that appropriate safeguards are in place to prevent any future breaches.

3.3 Either the Information & Privacy Department or Information Risk Management, as appropriate, shall investigate reported breaches in a timely manner and engage with other AHS program areas, including but not limited to, Human Resources, Ethics & Compliance, and Protective Services, as appropriate. Actions taken to correct breaches may include, but not be limited to recommendations for:

a) changes in policies, procedures, or practices;

b) education through in-service programs; and

c) disciplinary action up to and including dismissal.

3.4 Information Risk Management and the Information & Privacy Department shall jointly develop and manage incident response processes to respond to information and privacy breaches. Suspicious results, ranging from specific incidents to assessments of department processes, generated by audits of AHS information systems shall be investigated by Information Risk Management or the Information & Privacy Department, as appropriate. The investigations shall determine whether AHS information has been collected, used, disclosed, accessed, or disposed in accordance with applicable legislation, and AHS policies and procedures.

3.5 Information & Privacy shall report required health information breaches to the Office of the Information and Privacy Commissioner of Alberta in accordance with relevant legislation (as applicable).

DEFINITIONS

AHS people means Alberta Health Services employees, members of the medical and midwifery staffs, Students, Volunteers, and other persons acting on behalf of AHS (including contracted service providers as necessary).

Breach means a failure to observe security or privacy processes, procedures or policies, whether deliberate or accidental, which results in the information being viewed, or having the potential to be, accessed, used, transmitted or held by unauthorized persons.

Business information means general information, which is any recorded information about AHS' business activities such as those related to facilities, infrastructure, and security; policies and programs; budgets, expenses, and contracts; reports and statistics, etc., that are under the custody or control of AHS.

Health information means one or both of the following:

a) diagnostic, treatment and care information; and
b) registration information (e.g., demographics, residency, health services eligibility, or billing).

Personal information means recorded information, not governed by the *Health Information Act* (Alberta), of any kind stored in any format that identifies an individual including, but not limited to:

a) address and contact information (including an identifying number or symbol assigned to an individual);
b) race, ethnic origin, gender, or marital status;
c) educational, financial, employment, or criminal history;
d) opinions of others about the person;
e) the image of a person on a photograph; and
f) personal views and opinions of a person (except if these are about another person).

Repository owner means the individual(s) responsible for defining the processes and controls for the assessment, storage, security, privacy, and disposition of the information in a repository.

Security means the guarding or guaranteeing of the safety of AHS information and IT resources against misuse, theft or other dangers, and protecting the privacy and maintaining the integrity of information.

REFERENCES

- Alberta Health Services Governance Documents:
  - *Code of Conduct*
  - *Collection, Access, Use, and Disclosure of Information* Policy (#1112)
  - *Delegation of Authority and Responsibilities for Compliance with FOIP and the HIA* Policy (#1108)
  - *Information Classification* Policy (#1142)
  - *Information Technology Acceptable Use* Policy (#1109)
  - *Mobile Wireless Devices and Services* Policy (#1160)
  - *Monitoring and Auditing of IT Resources* Policy (#1144)
  - *Privacy Impact Assessments* Policy (#1145)
  - *Privacy Protection and Information Access* Policy (#1177)
  - *Whistleblower* Policy (#1101)

- Alberta Health Services Forms:
  - *Confidentiality and User Agreement* Form (#07922)
  - *Privacy Breach Notification* Form (#09579)
- Alberta Health Services Resources:
  - Access & Disclosure (Health Information Management): disclosure@ahs.ca
  - Information and Privacy: privacy@ahs.ca
  - Whistleblower Line (Confidential): 1-800-661-9675
- Non-Alberta Health Services Documents:
  - *Freedom of Information and Protection of Privacy Act* (Alberta)
  - *Health Information Act* (Alberta)

VERSION HISTORY

Date	Action Taken
October 16, 2019	Revised
Click here to enter a date	Optional: Choose an item