PURPOSE

- 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.

POLICY STATEMENT

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.

APPLICABILITY

Compliance with this policy is required by all AHS employees, members of the medical and midwifery staffs, students, volunteers, and other persons acting on behalf of AHS (including contracted services providers as necessary). This policy is subject to all applicable laws.

POLICY ELEMENTS

1. Training and Awareness

   1.1 The Information & Privacy Office and IT Security and Compliance shall provide education and training on information security and privacy principles (“information security and privacy training”) to ensure all staff and other persons acting on behalf of AHS 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 staff and other persons acting on behalf of AHS (including, but not limited to vendor representatives, students, and researchers) with access to AHS Restricted, Confidential, or Protected information (see Information Classification (#1142) policy) shall complete the provided information security and privacy training on commencement of their duties with AHS, and annually thereafter.

1.3 Persons 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 may have their access to information suspended until the training has been completed.

1.4 Upon appointment, Users 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 AHS Internal Audit may conduct audits of applicable AHS information security and privacy policies and risk management procedures. Recommendations from each audit shall be considered and, where appropriate, addressed by the AHS Information & Privacy Office and the IT Security and Compliance Office in collaboration with key stakeholders (e.g., Protection 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 Office and IT Security & Compliance Office for review; and
   b) address recommendations arising from the review.

3. Reporting and Responding to Breaches

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

3.2 AHS staff shall immediately report the Breach to the Information & Privacy Office or the IT Security or Compliance Office, as appropriate. When responding to a Breach, staff shall:

   a) cooperate with the assigned Information & Privacy or IT Security and Compliance 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 Office or IT Security and Compliance Office, 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 The IT Security and Compliance Office and the Information & Privacy Office shall jointly develop and manage incident response processes to respond to information privacy Breaches. Suspicious results, ranging from specific incidents to assessments of department standards or processes, generated by audits of AHS information systems shall be investigated by the IT Security and Compliance Office or the Information & Privacy Office, 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 The Information & Privacy Office may report Breaches to the Office of the Information and Privacy Commissioner of Alberta.

DEFINITIONS

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.

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

- AHS Code of Conduct
• AHS Policies:
  o Collection, Access, Use, and Disclosure of Information (#1112)
  o Delegation of Authority and Responsibilities for Compliance with FOIPP and the HIA (#1108)
  o Information Classification (#1142)
  o Information Technology Acceptable Use (#1109)
  o Monitoring and Auditing of IT Resources (#1144)
  o Privacy Impact Assessments (#1145)
  o Safe Disclosure/Whistleblower (#1101)
• Health Information Act (Alberta)
• Freedom of Information and Protection of Privacy Act (Alberta)

REVISIONS
None.