Alberta Health Services

# POLICY

**TITLE**
## INFORMATION TECHNOLOGY ACCEPTABLE USE

**SCOPE**
Provincial

**DOCUMENT #**
1109

**APPROVAL AUTHORITY**
Corporate Services Executive Committee

**INITIAL EFFECTIVE DATE**
June 24, 2009

**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 set out acceptable use of Alberta Health Services' (AHS) **information technology (IT) resources**.
- To maintain the integrity and **security** of IT resources.
- 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

The IT resources of AHS, including access to the internet and electronic forms of communication (e.g., email), are primarily intended for AHS business purposes. **Users** utilizing AHS IT resources shall comply with the AHS *Code of Conduct*, and applicable AHS policies, procedures, and standards including, but not limited to, those related to user IDs, passwords, email, information security, privacy, and confidentiality.

Users, as representatives of AHS, shall exercise careful judgment when using the internet, intranet, email, application access, or other AHS IT resources. The use of IT resources, the content of emails, information accessed via an application and other forms of communication may be audited or monitored, at the sole discretion of AHS without notice to users.

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. General Computing

1.1 Information Technology may at any time monitor, without notification to the user, all assigned user accounts and activities.

1.2 Users shall:

a) each be assigned a unique user ID to access IT resources;

b) be responsible for all actions taken by that user ID;

c) take necessary security precautions (e.g., protecting access to workstations) to prevent any user ID and/or password misuse; and

d) not allow another individual to use their user ID and/or password.

1.3 Users shall not remove or tamper with any IT resources, including hardware or software.

1.4 Users shall comply with the *Code of Behaviour for Computer Use* (see Appendix A below).

1.5 AHS IT resources shall not be used to conduct activities for private financial gain (see the *Conflict of Interest Bylaw*).

1.6 Users shall comply with the InfoCare behaviours, which include acting on need when collecting, accessing, using, and sharing only the personal, business, and health information that is required to perform the job duties and responsibilities as outlined in the *Privacy Protection and Information Access* Policy.

1.7 Users are prohibited from accessing or distributing illegal or objectionable material, including but not limited to:

a) obscene or pornographic material;

b) hate propaganda or discriminatory material;

c) defamatory and libellous material; and

d) sexually harassing material.

1.8 Copyrighted materials (such as third-party software) shall only be copied with a proper license or expressed written permission from the software manufacturer.

## 2. Electronic Communications

2.1 AHS owns all electronic communications, including those to social media sites, transmitted over AHS-owned IT resources. Users shall have no expectation of confidentiality regarding their electronic communications. AHS may access, monitor, block, and review these communications in accordance with applicable AHS policies, procedures, and standards, and/or legislation.

2.2 Electronic communications shall be subject to all applicable legislation and AHS policies, procedures, and standards.

2.3 Electronic communications containing any copyrighted information shall include the appropriate citations and acknowledgement of copyright. Any copyrighted information shall be used in accordance with applicable legislation.

2.4 Users shall not:

a) forge or attempt to forge email messages;

b) send or forward emails without a proper business function;

c) send illegal, harassing, objectionable, or threatening email messages;

d) transmit unsolicited information to multiple individuals unless it is for an authorized business function;

e) open attachments sent by unknown or suspicious parties;

f) send commercial advertisements or chain letters; or

g) create, modify, execute, or transmit any computer program or instructions intended to obscure the true identity of an email sender.

2.5 Encryption software, digital certificates, or secure protocols shall be used as required to protect email messages.

2.6 AHS electronic group mailing lists (i.e., lists allowing distribution of email messages to multiple recipients using a single address) shall be used for AHS business only. All group mailing lists shall have designated owners responsible for ensuring list-member accuracy.

2.7 Automatic email forwarding to sites outside of AHS is restricted to those approved by Information Technology.

## 3. Information Security

3.1 All electronic transmissions of **records**, including personal information or health information, shall be in compliance with the *Freedom of Information and Protection of Privacy Act* (Alberta), the *Health Information Act* (Alberta), and applicable AHS policies, procedures, and standards.

3.2 Transmission of information via email within the AHS-secured internal network shall occur only when there is a direct connection to the purpose for which the information was originally collected.

3.3 Transmission of personal information and identifiable health information by email to an external email account shall only occur if the information is encrypted and the recipient can be authenticated in accordance with the *Transmission of Information by Facsimile or Electronic Mail* Policy and the *Emailing Personal Identifiable Health Information* Procedure.

3.4 Transmission of personal information and health information via file transfer process shall only be through the secure AHS-implemented secure file transfer process.

## 4. Internet and Software Use

4.1 Reasonable personal use of AHS internet is permitted provided such use does not impact upon AHS' operational requirements and is in accordance with applicable legislation, the principles of the AHS *Code of Conduct*, and applicable AHS policies, procedures, and standards.

4.2 AHS internet shall not be used to conduct personal activities for private financial gain (see the *Conflict of Interest Bylaw*).

4.3 Accessing and using social media sites on IT resources for business purposes is permitted in accordance with the *Social Media* Policy.

4.4 Users shall not access or distribute illegal or objectionable internet material, including but not limited to:

a) obscene or pornographic material;

b) hate propaganda or discriminatory material;

c) defamatory and libellous material; and

d) sexually harassing material.

4.5 Users shall not, under any circumstances, personally install or download any software onto an IT resource. Users shall contact Information Technology when additional software is required. Approval of requests for additional software shall be based on business needs.

4.6 Information Technology shall monitor and assess risks posed to AHS by the use of the internet and shall disable access to any site/platform where there is reason to believe AHS systems or data are at risk.

## 5. IT Security and Compliance

5.1 AHS shall make all reasonable efforts to protect its IT resources from tampering, unauthorized access, and loss. Users shall comply with AHS policies, procedures, and standards to ensure the protection and security of AHS information and IT resources.

5.2 Users shall not interfere with or disrupt IT resources or other users, through actions including, but not limited to, the propagation of computer malware, the disconnection or damage to equipment and services, or other malicious activities.

5.3 Use of IT resources to gain or attempt to gain unauthorized access to information, services, or other resources within or outside AHS is strictly prohibited.

## 6. Mobile Wireless Devices, Laptops, and Mobile Storage Devices

6.1 Users shall be responsible for the security and protection of AHS information and IT resources in their possession. To minimize the risk of theft of **mobile wireless devices**, laptops, and **mobile storage devices** and the information carried therein, users shall:

a) restrict physical access to the mobile wireless devices, laptops, and mobile storage devices whenever possible (e.g., use cable locks for laptops to limit the likelihood of theft);

b) ensure that mobile wireless devices, laptops, and mobile storage devices remain in the user's possession at all times, in accordance with AHS policies, procedures, and standards;

c) not use automatic login processes (e.g., automatic password saving); and

d) store them in a secure location out of sight (e.g., in a locked file drawer) when not in use.

6.2 All mobile wireless devices, laptops, and mobile storage devices must use encryption in accordance with AHS policies, procedures, and standards to ensure the confidentiality and integrity of the stored information.

## 7. Compliance

7.1 Use of IT resources constitutes acceptance of compliance responsibilities identified in agreements signed upon appointment and applicable AHS policies, procedures, and standards. Failure to abide by the agreement and applicable AHS policies, procedures, and standards, or using AHS IT resources

inappropriately shall be grounds for disciplinary action up to and including dismissal. Where illegal activities have occurred, the appropriate authorities shall be notified.

## 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).

**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).

**Information technology (IT) resource** means any AHS-owned or controlled asset used to generate, process, transmit, store, or access AHS information, which includes but is not limited to IT infrastructure, computer facilities, systems, hardware, software, information systems, networks, shared drives, computer equipment and devices, internet, email, databases, applications, mobile wireless devices, and mobile storage devices.

**Mobile storage device** means portable devices used to store data including but not limited to analog or digital voice recorders, external hard drives, memory cards, flash and other data storage drives, optical storage devices (e.g., CDs, DVDs, and Blu-ray discs), and other similar devices.

**Mobile wireless devices** means smartphones, cellular phones, tablet computers (e.g., iPads) excluding laptop computers, wireless data cards (air-cards), mobile data terminals (MDT), two-way radios, and pagers.

**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).

**Record** means documents, data or information of any kind, in any medium (e.g., paper, digital, and audio-visual media), and in any format (e.g., documents, spread sheets, databases, emails, blogs, wikis, and website pages) created, received, recorded, and maintained by Alberta Health Services as part of its services or business. This definition includes health records, but does not include computer software or any mechanisms that produce records.

**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.

**User** means any person who accesses or uses an IT resource.

## REFERENCES

- Appendix A: *Code of Behaviour for Computer Use*
- Alberta Health Services Governance Documents:
  - *Access to Information (Physical, Electronic, Remote)* Policy (#1105)
  - *Code of Conduct*
  - *Collection, Access, Use, and Disclosure of Information* Policy (#1112)
  - *Contractor Requirements for Security and Privacy of Information and Information Technology Resources* Policy (#1107)
  - *Delegation of Authority and Responsibilities for Compliance with FOIP and the HIA* Policy (#1108)
  - *Emailing Personal Identifiable Health Information* Procedure (#1113-01)
  - *Information Security and Privacy Safeguards* Policy (#1143)
  - *Mobile Wireless Devices and Services* Policy (#1160)
  - *Official Records Destruction* Procedure (#1133-02)
  - *Privacy Protection and Information Access* Policy (#1177)
  - *Progressive Discipline Procedure* (#1116-05)
  - *Records Management* Policy (#1133)
  - *Records Retention* Schedule (#1133-01)
  - *Transitory Records* Procedure (#1133-03)
  - *Transmission of Information by Facsimile or Electronic Mail* Policy (#1113)
  - *Whistleblower* Policy (#1101)
- Non-Alberta Health Services Documents:
  - *Freedom of Information and Protection of Privacy Act* (Alberta)
  - *Health Information Act* (Alberta)

## VERSION HISTORY

| Date | Action Taken |
|---|---|
| January 10, 2012 | Revised |
| October 16, 2019 | Revised |
| Click here to enter a date | Optional: Choose an item |

**APPENDIX A**

## Code of Behaviour for Computer Use

1. **Personal Responsibility and Accountability**
   All users shall be personally responsible and accountable for all activities undertaken under their assigned credentials/user ID. Where it is suspected that credentials/user ID are lost or compromised, users shall immediately notify the AHS IT Service Desk for assistance and direction. The Service Desk shall report the matter to Information Risk Management for investigation.

2. **Access to IT Resources**
   Explicit authorization is required for access to IT resources. Unauthorized use of IT resources, or use of false or misleading information to gain use of these resources, is strictly prohibited. IT resources shall not be used to gain unauthorized access to other individuals', organizations', or institutions' computing facilities and technology.

3. **Usage of IT Resources**
   AHS' IT resources are primarily intended for AHS business purposes. Using AHS' IT resources to conduct activities for private financial gain is not permitted. Additionally, users must not:

   - permanently or temporarily alter or interfere with the standard configuration, operation, or procedures related to IT resources through personally installing or downloading software onto an IT resource; and
   - negatively impact the operational requirements of AHS or alter the performance of AHS computer networks and/or connected devices.

4. **Sharing of Passwords or User IDs**
   Sharing of passwords or allowing other individuals to use a users' unique user ID is prohibited. Users shall take reasonable precautions to protect the privileges assigned to them and ensure terminals or workstations are logged-off when left unattended or not in use.

5. **Software Piracy and Use**
   Users shall ensure software is legally copied and used in accordance with its license.

6. **Regular Computer Reboots**
   Computing devices connecting to AHS networks must use a standard anti-virus product approved by the Information Risk Management. It is strongly recommended that users reboot a minimum of once per week to ensure virus protection and patch updates.

7. **Use of AHS Email Accounts**
   Email is a corporate resource. AHS owns all email transmissions on AHS networks and shall monitor email accounts as required. Users' emails are not private and users should not expect that their emails are private. Email transmissions may be subject to public disclosure in accordance with applicable legislation. All electronic transmissions (including, but not

limited to emails, texts, and transmissions to social media sites) of AHS information shall be in accordance with applicable legislation and AHS policies.

**8. Need to Know**

Users shall access the minimum information necessary through IT resources to fulfil their duties on behalf of AHS, and shall only share the minimum information necessary through IT resources with colleagues or other AHS people as necessary to fulfil their AHS-related duties. Users shall only access information or records through IT resources as required to fulfill their AHS duties. Users shall only access patient and health information through IT resources where:

a) they are on the patient's treatment team; or
b) it is required in the course of their duties.

**9. Protection and Privacy of Information**

Users shall maintain and protect the confidentiality of any and all information accessed through the use of IT resources. Users shall take steps to safeguard against unauthorized access, as well as report improper activities.

**10. Storage of Electronic Information**

All AHS electronic information is owned by AHS and shall be stored on AHS protected network drives which have proper access controls to ensure only authorized access. Storing AHS electronic information on workstations or memory devices and electronic devices is not permitted unless specifically authorized by Information Risk Management and the information is encrypted according to AHS policies, procedures, and standards.

**11. Reporting Improper Activities**

Users shall immediately report improper activities or any activity which is perceived to be improper on IT resources to the AHS IT Service Desk. The Service Desk shall report the matter to Information Risk Management for investigation. Improper activities, or activities which are perceived to be improper that involve information, shall be reported to the AHS Information & Privacy Department.