Alberta Health Services

POLICY

TITLE
MOBILE WIRELESS DEVICES AND SERVICES

SCOPE
Provincial

DOCUMENT #
1160

APPROVAL AUTHORITY
Alberta Health Services Executive

INITIAL EFFECTIVE DATE
February 4, 2015

SPONSOR
Information Technology

REVISION EFFECTIVE DATE
January 12, 2021

PARENT DOCUMENT TITLE, TYPE, AND NUMBER
Not applicable

SCHEDULED REVIEW DATE
January 12, 2024

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 Policy Services at policy@ahs.ca. The Policy Services website is the official source of current approved policies, procedures, directives, standards, protocols, and guidelines.

OBJECTIVES

- To outline the allocation and acceptable use of **mobile wireless devices** used to access Alberta Health Services (AHS) **information technology (IT) resources**.
- To outline the eligibility and criteria for use of mobile wireless devices in the AHS Bring Your Own Device (BYOD) program.
- To provide **AHS people** with an understanding of the criteria employed in the procurement and allocation of AHS-owned mobile wireless devices, and direction on their accepted use for health care delivery and business services.
- To protect information in the custody or control of AHS while being transmitted and/or stored on mobile wireless devices.

PRINCIPLES

AHS recognizes the vital role mobile wireless devices play in the access, use, and transmission of information for health care delivery and business services.

All mobile wireless devices used to access AHS resources shall comply with applicable legislation, the AHS *Code of Conduct*, and AHS bylaws, policies, and procedures.

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 Principles

1.1 This Policy applies to the following mobile wireless devices:

a) AHS-owned mobile wireless devices, which are mobile wireless devices owned by AHS and allocated to AHS people, or others, for the purposes of supporting a business function. These devices contain security functionality permitting them to connect to the AHS IT resources (e.g., AHS' secure **wi-fi**) in accordance with this Policy, other applicable AHS policies, and AHS' security requirements. AHS has full authority and governance over security controls on AHS-owned mobile wireless devices.

b) Mobile wireless devices enrolled in the AHS Bring Your Own Device (BYOD) program, which are mobile wireless devices owned by an AHS person or a professional corporation which have AHS-sanctioned security features implemented on them for the purposes of connecting to AHS IT resources in accordance with this Policy, other applicable AHS policies, and AHS' security requirements. AHS has limited authority and governance over security controls for mobile wireless devices enrolled in BYOD program.

c) Personal mobile wireless devices, which are owned by an AHS person, another individual, or a professional corporation that have no AHS-sanctioned security features. These mobile wireless devices are not permitted to access AHS' network environment (e.g., are limited to using AHS public networks for patients and visitors).

1.2 Several sections of this Policy apply to only one, or a few, of the mobile wireless devices above. Any sections which reference specific types of mobile wireless devices apply to only those types of mobile wireless devices. Any references to 'mobile wireless devices' in general throughout this Policy apply to all types of mobile wireless devices.

2. Eligibility and Allocation for AHS-Owned Mobile Wireless Devices

2.1 An AHS-owned mobile wireless device may be issued to AHS people upon appropriate approval.

a) All requests for AHS-owned mobile wireless devices shall be approved by appropriate AHS management (minimum, Executive Director), and requested through the Information Technology (IT) Customer Service Portal.

b) IT Leadership and AHS Executive Leadership have the ability to deny or restrict the approval of new requests (as outlined in Section 2.1(a) above) for AHS-owned mobile wireless devices based on budget availability and

other considerations set out by IT Leadership and the AHS Executive Leadership.

2.2 Approval, as set out in Section 2.1 above, may be based on one or more of the following business needs:

a) Member of Executive/Senior Leadership Team and their support staff who are required to be readily accessible on short notice.

b) AHS people who are required to utilize mobile wireless device(s) as part of their job responsibilities.

c) AHS people who are frequently away from the office due to job responsibilities.

d) AHS people who are a key contact during an emergency (e.g. Business Continuity Representative).

e) AHS people who require a mobile wireless device for safety reasons due to job responsibilities or working conditions (e.g. remote care worker, frequent traveller, work alone, perform hazardous work).

f) Required by Management/Supervisor as part of a work or on-call responsibility.

2.3 Situations where there should be consideration of transferring or returning an AHS-owned mobile wireless device includes the following:

a) Should **users** move to a new team within AHS, the former and current managers shall determine if/what related AHS-owned mobile wireless device(s) should remain with the team or follow the user in their new role.

b) Should a user leave AHS, their AHS-owned mobile wireless device(s) may be transferred to a new AHS person assuming the role, or returned to AHS IT Mobility Services for reallocation.

(i) When transferring an AHS-owned mobile wireless device, the new user shall contact the IT Service Desk to initiate reconfiguration of the mobile wireless device(s) and carrier settings by AHS IT Mobility Services.

c) AHS-owned mobile wireless device(s) no longer required shall be returned to AHS IT Mobility Services at an address provided on the AHS IT Mobility Services Support page on Insite.

3. International Roaming

3.1 By default, international roaming is disabled on all AHS-owned mobile wireless devices.

3.2 Personally funded international roaming options are not available to users. Users may purchase a SIM card at their destination of travel as an alternative. Contact AHS IT Mobility Services for more information.

3.3 Roaming charges incurred while on any type of leave require reimbursement to AHS by the user, with the exception of users who are on call during the leave (see Section 3.4 and 3.5 below).

3.4 AHS-owned mobile wireless device usage for out-of-country business travel shall be approved prior to travel taking place:

a) A person at a Vice President level, or higher does not require approval for out of country business travel use of an AHS-owned mobile wireless device, but shall contact AHS IT Mobility Services to request an international roaming package no less than seven (7) business days prior to travel.

b) Other users shall request and receive Vice President approval for out of country business travel use of an AHS-owned mobile wireless device, and contact AHS IT Mobility Services after approval to request an international roaming package no less than seven (7) business days prior to travel.

3.5 When travelling outside of Canada with an AHS-owned mobile wireless device, including travel to the United States, it is the responsibility of AHS people to read and comply with the *Travelling with Your AHS Mobile Device* guide provided on Insite, be attentive to international data roaming charges which can be significant, and use Wi-Fi wherever available. Use of data for personal reasons when roaming internationally, and especially with bandwidth intensive applications, can result in significant data charges. AHS people shall be required to reimburse AHS for charges related to personal use while traveling.

4. Bring Your Own Device Eligibility and Criteria for Use

4.1 Individuals and devices eligible for the AHS BYOD program are set by IT in the AHS *BYOD Framework* and are subject to change.

4.2 Mobile wireless devices enrolled in the BYOD program shall have applicable security controls (i.e., enterprise mobile management) authorized by IT installed on their mobile wireless device in order to access AHS IT resources. Access to AHS IT resources on a mobile wireless device enrolled in the BYOD program shall only occur using these security controls.

4.3 AHS people who have been approved to enroll in the BYOD program shall be required to accept any terms of use applicable to all the security control platforms within the scope of BYOD, and any additional terms of use established by AHS, before they can use their mobile wireless device enrolled in the BYOD program to access AHS IT resources.

4.4 Use by AHS people of a mobile wireless device enrolled in the BYOD program is subject to:

a) the *Health Information Act* (Alberta), *Freedom of Information and Protection of Privacy Act* (Alberta), and other applicable legislation and regulations;

b) this Policy, the *BYOD Framework, and the Bring Your Own Device ("BYOD") Terms and Conditions*;

c) all applicable AHS bylaws, policies, procedures, directives, standards, guidelines, and protocols, notably, the AHS *Privacy Protection and Information Access* Policy, the *IT Acceptable Use* Policy, and other AHS information security and privacy policies; and

d) the terms of use set out the mobile wireless device manufacturer and the applicable security control platforms required to access AHS IT resources.

4.5 AHS people with mobile wireless devices enrolled in the BYOD program are responsible to:

a) maintain the security and confidentiality of the information accessed on the mobile wireless device enrolled in the BYOD program;

b) secure the mobile wireless device enrolled in the BYOD program from unauthorized access;

c) ensure only the enrolled user can access AHS resources on the mobile wireless device enrolled in the BYOD program (for instance, not having AHS user names and passwords auto filled, ensuring inactivity lockouts are enabled);

d) ensure that **personal information**, **health information**, or **business information** in the custody or control of AHS is saved on the mobile wireless device enrolled in the BYOD program only within the authorized security control platforms as outlined in Section 4.2 above;

e) ensure any features or tools on the mobile wireless device enrolled in the BYOD program are enabled or disabled, as directed by IT; and

f) ensure the applicable security control platforms and operating system are kept up-to-date on the mobile wireless device enrolled in the BYOD program.

4.6 Information Technology is responsible for:

a) managing access to the BYOD program;

b) managing and maintaining the *BYOD Framework*;

c) providing direction to users on required security controls, encryption, and other security practices necessary to protect the mobile wireless device enrolled in the BYOD program from unauthorized access;

d) supporting users when a mobile wireless device enrolled in the BYOD program has been lost or stolen, including any necessary data wipes and/or breach reporting;

e) providing support for the BYOD program, excluding any technical support on the device itself or the user's service plan with their provider; and

f) monitoring and auditing functions in accordance with the *Monitoring and Auditing of Information Technology Resources* Policy.

4.7 AHS, or applicable security control platforms, may need to send the user updates through the mobile wireless device enrolled in the BYOD program in order to provide BYOD program information, software update notifications, or other important messages. Users shall enable notifications for these updates.

4.8 Mobile wireless devices enrolled in the BYOD program are not eligible for reimbursement for business calls, data, or any other expenses outlined in Section 11 below.

4.9 Failure to comply with the above requirements may result in removal from the BYOD program and disciplinary action.

5. Mobile Wireless Device Education for Users

5.1 All AHS people who are authorized and assigned the use of an AHS-owned mobile wireless device, or a mobile wireless device enrolled in the BYOD program, are required to be fully familiar with, and follow the appropriate terms of use of their device (e.g., software licences, hardware licences) as it pertains to AHS.

5.2 All AHS people using any mobile wireless device for AHS business purposes are expected to understand and follow applicable policies, documentation, suggested readings, and self-education resources listed in the References section of this Policy, and related resources provided on the AHS IT Mobility Services home page on Insite.

6. Information Security and Privacy

6.1 Health, personal, and business information in the custody or control of AHS is not to be collected, accessed, transmitted, or stored on mobile wireless devices unless the mobile wireless device meets the information security requirements outlined in the *Information Technology (IT) Acceptable Use* Policy and other applicable AHS policies, procedures, and standards.

6.2 Collection, access, disclosure, transmission, and storage of information in the custody or control of AHS on a mobile wireless device shall be in accordance

with the *Health Information Act* (HIA) (Alberta), the *Freedom of Information and Protection of Privacy Act* (FOIP) (Alberta), and applicable AHS policies.

6.3 Health, personal, and business information in the custody or control of AHS may only be transmitted from a mobile wireless device if the transmission is in accordance with the requirements in the HIA, FOIP, and applicable AHS policies. This includes transmission by **Short Message Service** (SMS or Text Messaging), **Multimedia Messaging Service** (MMS), or any other messaging application (including email). Transmission of personal, health, and business information in the custody or control of AHS must meet or exceed the encryption and information security standards in place for transmission of information by electronic mail as set out in the *Transmission of Information by Facsimile and Electronic Mail* Policy and the *Emailing Personal Identifiable Information* Procedure.

6.4 Mobile wireless device users shall take reasonable precautions when making a call or viewing information on a mobile wireless device to ensure that individually-identifying health information, individually-identifying personal information, and business information in the custody or control of AHS cannot be overheard and/or viewed by unauthorized parties.

7. Photography, Videos, and Audio, and Video Recordings

7.1 All photographs, videos, and/or audio recordings used to collect health, personal, and business information shall be collected, access, used, disclosed, and managed in accordance with FOIP, HIA, and AHS policies and procedures.

7.2 Verbal consent shall be obtained and recorded for the collection of health information by photograph, video, or audio recording.

a) Should the recording device not be obvious to the patient for a purpose authorized under the HIA, written consent shall be obtained using the *Consent to collection and use of a recording device or camera for Photographs, Video or Sound Recordings for Health Care purposes* Form.

7.3 Photographs, videos, or audio recordings used for media, promotions, publications, education, presentations, and other similar purposes shall have the consent of the individuals appearing in the recording. The consent shall be obtained using the *Consent To Collect, Use, and Disclose Stories, Photos and/or Video and Sound Recordings* Form.

7.4 Photographs, videos, or audio recordings containing health, personal, or business information are considered records and shall be managed in accordance with the *Records Management* Policy and associated procedures.

7.5 Mobile wireless devices used to take photographs, videos, or audio recordings containing health, business, or personal information shall not be synced to any

cloud storage system, unless otherwise authorized by Information Risk Management.

7.6 Where practical, all photographs, videos, and audio recordings should be non-identifiable.

7.7 Photography, audio, or video recordings not containing health, personal, or business information are to be managed in accordance with the AHS *Privacy Protection and Information Access* Policy and other AHS privacy policies and procedures.

8. Use of Mobile Wireless Devices in AHS Facilities

8.1 Reasonable use of personal mobile wireless device(s) is permitted in AHS facilities in accordance with the principles of the *Code of Conduct* and applicable policies and procedures.

8.2 AHS people shall be considerate of their surroundings and respect others' privacy and safety when using a mobile wireless device in AHS facilities.

9. Personal Use of AHS-Owned Mobile Wireless Devices

9.1 Personal use of an AHS-owned mobile wireless devices includes, but is not limited to voice, texting, data usage, downloading and utilizing applications, and long distance calling. AHS reserves the right to audit, store, or review all uses and data stored on AHS-owned mobile wireless devices.

9.2 AHS-owned mobile wireless devices provided by AHS IT Mobility Services are the property of AHS. AHS people may use AHS-owned mobile wireless devices for personal use provided that such use:

a) protects the confidentiality, integrity, and security of health, personal, and business information and other AHS proprietary assets;

b) does not interfere in the performance of their employment or contractual duties;

c) does not appear to speak on behalf of, or in representation of AHS without appropriate approvals;

d) are not used to transmit or send inappropriate, improper, annoying, excessive, threatening, or obscene material or to otherwise harass, offend, threaten, embarrass, distress, or invade the privacy of any individual or entity;

e) is used in accordance with the *IT Acceptable Use* Policy;

f) does not result in a net material cost to the organization;

g) is consistent with professional conduct;

h) is not for personal or financial gain in accordance with the *Conflict of Interest Bylaw*; and

i) does not cause support issues from the use of non-business related applications.

9.3 Excessive charges on an AHS-owned mobile wireless device may require reimbursement by the user.

9.4 AHS-owned mobile wireless devices shall not be loaned or shared with others, including friends or family. Usage is the responsibility of the AHS person assigned to the device.

9.5 While AHS people may use AHS-owned mobile wireless devices for personal use, in some cases, an AHS person may be required to reimburse AHS for:

a) personal long distance charges; and/or

b) minutes, text, data usage (e.g., streaming video/music), or premium-rate telephone number fees (e.g., chat lines, competitions or voting).

10. Lost or Stolen Mobile Wireless Device

10.1 If an AHS-owned mobile wireless device, or a mobile wireless device enrolled in the BYOD program, is lost or stolen, the user shall report the incident immediately to the IT Service Desk. The IT Service Desk shall alert Information Risk Management for a follow-up investigation, and if appropriate, Information Risk Management shall notify Information & Privacy in accordance with AHS *Privacy Protection and Information Access* Policy and *Information Security & Privacy Safeguards* Policy.

11. Reimbursement of AHS Business Calls Made from Personal Devices

11.1 AHS people may be eligible to request reimbursement for business calls made on their personal mobile wireless device. Written approval from the AHS person's direct supervisor (minimum, Executive Director and subject to the limits in the *Delegation of Approval Authority* Policy) shall be obtained before the expense can be incurred. A copy of the approval and documentation of the incurred charges shall be included with the AHS person's expense claim.

11.2 AHS people eligible to claim reimbursement for business calls made on their personal mobile wireless device (in accordance with Section 11.1 above) shall provide proper documentation indicating they incurred a charge for the business call and submit their claim for reimbursement using an expense claim. Reimbursement shall not be made if the business calls were made within a period of unlimited usage included in the rate plan, or where reasonable cost-free alternatives exist.

12. Mobile Wireless Device Use While Driving a Vehicle

12.1 In accordance with the *Distracted Driving Regulation* (Alberta), a driver shall use hands-free 'one-touch' or voice activated functions and not hold, view, or manipulate a mobile wireless device that can send or receive phone calls, electronic data, electronic mail, or text messages while the vehicle is in motion.

12.2 Emergency Medical Services (EMS) health care providers are expected to comply with all of the required standards and expectations and outlined in the *Operating Emergency Medical Services Vehicles* Policy.

13. Infection Prevention and Control for Mobile Wireless Devices

13.1 Mobile wireless devices used by AHS people in health care settings shall be cleaned and disinfected in accordance with the Infection Prevention & Control (IPC) Best Practice Guidelines.

DEFINITIONS

AHS people means AHS 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 resource (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 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.

Multimedia Messaging Service (MMS) means a technology which enables mobile devices to exchange messages which include a variety of media, such as photos, video, and audio. MMS can also deliver text-based messages greater than 160 characters in length. MMS operates via a Mobile Wireless Network.

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).

Short Message Service (SMS) means a technology that enables mobile devices to exchange short text-based messages of 160 characters or less via a Mobile Wireless Network.

User means an individual who operates a mobile wireless device.

Wi-Fi means a technology allowing devices equipped with the required components to communicate with one another wirelessly in a particular area.

REFERENCES

- Alberta Health Services Governance Documents:
  - *Code of Conduct*
  - *Conflict of Interest* Bylaw
  - *Access to Information (Physical, Electronic, Remote)* (#1105)
  - *Information Security & Privacy Safeguards* Policy (#1143)
  - *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 Approval Authority* Policy (#1168)
  - *Information Classification* Policy (#1142)
  - *Information Technology Acceptable Use* Policy (#1109)
  - *Monitoring and Auditing of Information Technology Resources* Policy (#1144)
  - *Non-Identifying Health Information Standard (IPO-2013-0004)*
  - *Privacy Protection and Information Access* Policy (#1177)
  - *Records Management* Policy *(#1133)*
  - *Transmission of Information by Facsimile and Electronic Mail* Policy (#1113)
  - *Travel, Hospitality & Working Session Expenses – Approval, Reimbursement & Disclosure* Policy (#1122)
  - *Operating Emergency Medical Services Vehicles* Policy (#PS-EMS-01)
- Alberta Health Services Forms
  - *Consent to collection and use of a recording device or camera for Photographs, Video or Sound Recordings for Health Care purposes* Form
  - *Consent To Collect, Use, and Disclose Stories, Photos and/or Video and Sound Recordings* Form
- Alberta Health Services Resources:
  - *Bring Your Own Device (BYOD)* Framework
  - *Bring Your Own Device ("BYOD") Terms and Conditions*

- *Freedom of Information and Protection of Privacy Act (FOIP) and Health Information Act (HIA) Information for AHS staff*
- *Guidance for Staff Regarding Audio Video Recordings*
- Infection Prevention & Control (IPC) Best Practice Guideline: *Cleaning and Disinfection of IT Equipment*
- *AHS Mobile Device Guidelines for Travelling*
- *Self-Help Information for Users of AHS Mobile Devices*

- Non-Alberta Health Services Documents:
  - *Distracted Driving Regulation* (Alberta)
  - *Freedom of Information and Protection of Privacy Act* (Alberta)
  - *Health Information Act* (Alberta)
  - *Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization?* (Office of the Information and Privacy Commissioner of Alberta)
  - *Traffic Safety Act* (Alberta)