Mobile Device Usage Policy

Category:	Academic
Number:	TBA
Responsibility:	Associate Dean, Undergraduate Medical Education
Approval:	Student Academic Management Committee
Date:	September 21, 2021 revision approved October 12, 2021 Review: October 2023

Purpose:

The purpose of the *Mobile Device Usage Policy* is to prescribe college-level standards, responsibilities and restrictions on the use of mobile devices by medical students when they are in clinical learning experiences including clerkship rotations and clinical electives. The policy also seeks to balance the risk of access to confidential patient information with the learning needs of the medical students.

This policy is aligned with Schedule N of the Clinical Placement Agreement (CPA) which was developed by the Saskatchewan Academic Health Sciences Network and which went into effect on May 1, 2017. The CPA is a binding agreement between the College of Medicine, University of Saskatchewan, Saskatchewan Health Authority (SHA) formerly referred to as the Regional Health Authorities (RHAs) and the Saskatchewan Cancer Agency.

Principles:

Responsibility: The *Mobile Device Usage Policy* establishes clear responsibilities for medical students, residents and clinical faculty in the Undergraduate Medical Education program.

Definitions:

App: an application that is typically a small specialized program downloaded to a mobile device.

Mobile Device: a laptop computer or a pocket-sized computing device (a device typically having a display screen with touch input or a miniature keyboard that can store electronic data files and software). A mobile device includes but is not limited to: laptop computer, tablet computer, personal digital assistant (PDA), cellular phone, smart phone, smartwatch, and ultra-mobile PC (UMPC). This includes home PCs and personal mobile devices used to access SHA/SCA's network, data, or applications.

Patients: the recipient of health care services or consultations provided by the SHA/SCA. This term includes clients and long-term care residents.

Personal Health Information (PHI) means, with respect to an individual, whether living or deceased:

- information with respect to the physical or mental health of an individual;
- information with respect to any health service provided to an individual;
- information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
- information that is collected: (A) in the course of providing health services to the individual; or (B) incidentally to the provision of health services to the individual; or
- registration information;
- images including photographs

Saskatchewan Health Authority (SHA) formerly referred to as the Regional Health Authorities (RHAs): as defined by The Provincial Health Authority Act, provide most health services in Saskatchewan, either directly or through affiliated health care organizations.

Remote Access: communication with a health authority information system or network using a mobile device from a remote location or facility through a public-accessible data link (e.g. Internet or modem). Some of the more common methods of providing this type of remote access are: remote dial-in through a modem, virtual desktop, login through the Internet (with programs or apps such as Citrix), Outlook Web access and remote email/calendar synchronization via the cellular network.

Removable Media: storage media that can store electronic data files or software and be removed from its device reader. Removable media includes, but is not limited to: memory cards, USB flash drives, pens that digitally record data, CDROMs, DVDs, or data backup or storage tapes.

SHA/SCA information system: to any system that captures, stores, manages or transmits information related to the health of individuals or the activities of organizations that work within the health sector.

Saskatchewan Cancer Agency (SCA) is responsible for the planning, organization, delivery and evaluation of cancer care and related health services throughout the province.

Unsecure Network: a wireless network that you can access without entering a password. Wireless connections available in cafés or from creating a local “hotspot” with a personal phone are examples of unsecure networks.

Scope of this Policy:

This policy applies to all undergraduate students registered in the Doctor of Medicine (MD) program at the University of Saskatchewan irrespective of the geographically distributed site/campus to which they are currently assigned as well as residents and clinical faculty.

Policy:

1.0 Mobile Device Modification and Usage

- Students will not use personal devices to access PHI in SHA/SCA data systems unless pre-authorized by their education programs and the Information Technology (IT) department within the SHA/SCA in which they will be accessing information and data systems.

- Students can use personal or SHA/SCA provided mobile devices in clinical areas to research health information on the internet or connect to course required apps for purposes of providing health services to patients or for learning needs or course requirements specific to their placement learning objectives. Use of mobile devices for personal reasons should be conducted away from clinical areas and should be limited to break times except in emergencies. Use of mobile devices in clinical areas should never interfere with patient care or negatively impact the perception of services being offered to the patient. Whenever possible students should have their personal phones set to silent or vibrate unless they are required to be available to a supervisor.

- Students are never permitted to use non-SHA/SCA email accounts for communicating PHI. Communication via email of PHI may only be done between two email accounts from the same organization; inter-SHA/SCA emailing of PHI is not permitted.

- Mobile devices provided by the health authority to a student will be subject to all policies of the SHA/SCA related to mobile devices including password protection, internet acceptable use and privacy and confidentiality.

- Students that are granted remote access to SHA/SCA information systems from a personal device for patient care or course requirements must abide by the SHA/SCA policies and procedures regarding access to information systems including policies and procedures on remote access to information systems and password protection. Personal devices used in this manner must also employ any security measures deemed necessary by the SHA's/SCA's IT department. SHAs/SCA may require students to complete an application form to be granted remote access on personal devices.

- Students shall never make modifications, disable or tamper with SHA/SCA owned and installed hardware or software configurations. This includes, but is not limited to: data encryption, screen-saver passwords and anti-virus software.

- Students shall never install any software on SHA/SCA mobile devices without prior authorization.

2.0 Storage of PHI on Mobile Devices

- Students shall never permanently store information from a SHA/SCA information system or PHI (including photos, video or audio recordings, or text messages) on a mobile device or removable media. This information must be saved as appropriate to the SHA/SCA network or information system (or otherwise added to the patient's chart or record of care) and permanently removed from the mobile device or media as soon as possible. Saved images must follow the consent policies and procedures of the SHA/SCA.

- Students will not take photos, videos or audio recordings of patients, including close up pictures of wound, rashes, etc. except in exceptional circumstances when required by their supervisor for the immediate care of a patient. *Photographs and PHI cannot be shared through an unsecure network (e.g. texting).*

3.0 Communication of PHI between users

- PHI (e.g. text, photos, videos, or audio recordings) may only be communicated between mobile devices via texting if students utilize a secure, SHA/SCA-hosted messaging service (i.e. messages in transit are encrypted; photos taken are taken within an app and not inadvertently accessible, shared, or synced with the phone's default photo library or cloud; and the SHA/SCA hosts/controls the messaging server). If in doubt, students shall consult their SHA/SCA IT department and Privacy Officer.

- An insecure medium (e.g. texting, emails other than between two email addresses from the same SHA/SCA) may only be used to communicate PHI (text, photos, videos, or audio recordings) in the following circumstances:
    - The patient or legal guardian has provided informed written or verbal consent (he/she must have had the risks explained to them), or
    - It is an emergency situation where the benefit to patient outweighs the risks.

- Always consider if there is another more secure, reliable, or timely mechanism that can be used (e.g. referring others to existing PHI as stored within a SHA/SCA clinical application); when in doubt, students shall revert to safer modes of communication. When information, in the student's best judgment, must be sent insecurely, students shall document this decision and their rationale, shall only include the minimum amount of PHI necessary to meet the recipient's needs, and must ensure that the information reached the intended recipient, is being handled with appropriate care and is deleted by the recipient immediately afterwards.

- Students will not take pictures of other students or staff in the clinical setting or pictures of the clinical setting itself unless permission has been obtained from the clinical supervisor and from those in the picture. Photographs taken must not include any patients (including in the background).

4.0 Infection Control

- All touch surfaces of IT devices used at, or near, point of care must be cleaned and disinfected (per manufacturer's instructions) with a hospital-grade disinfectant if used or touched during the encounter with the patient.

- Students using their own device or assigned a device from the SHA/SCA are responsible for routine cleaning and disinfection of the device.

- Devices that cannot be adequately cleaned and disinfected should not be used during placements.

5.0. Responsibilities of the Students

- Abide by the terms of this agreement and any additional policies or procedures deemed relevant by the SHA/SCA in which they are placed.

- Employ expected physical security measures for any mobile device or removable media used for SHA/SCA business, especially when they contain SHA/SCA data. This applies whether or not the devices are actually in use and/or being carried. This includes, but is not limited to passwords, encryption, and physical control of such devices (e.g. securing laptops at workstations or in offices with a cable lock).

- Immediately report lost or stolen mobile devices or removable media to their Manager and/or as required by their respective SHA/SCA policy and procedures.

- Immediately report any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of SHA/SCA resources, databases, networks, etc. to their SHA/SCA supervisor and program instructor and/or as required by SHA/SCA policy and procedures.

- Return SHA/SCA mobile devices to a manager/director/supervisor or designate when no longer needed or when the clinical placement is complete. Non-SHA/SCA devices that no longer require access to a SHA's/SCA's network, applications or data must be wiped clean of all information related to the clinical experience including information regarding SHA/SCA information systems and PHI and/or reset to factory settings. If uncertain on how to do this, contact the SHA's/SCA's IT department for assistance.

- Regularly disinfect devices, and disinfect after use at point of care, or near care.

6.0 Consequences for Noncompliance

- Non-compliance with this policy will result in a review of the incident by the SHA/SCA and the educational institution. A review of non-compliance may result in:

    - Temporary or permanent loss of privileges for access to some or all computing and networking resources and facilities.

- Disciplinary action by the manager, up to and including termination of the placement by the SHA/SCA or educational institution.

- Legal action according to applicable federal and provincial laws and contractual agreements.

Responsibilities

The Associate Dean, Undergraduate Medical Education, is responsible for providing oversight to the overall administration of the *Mobile Device Usage Policy.*

The Manager, Undergraduate Medical Education, with the assistance of the Undergraduate Medical Education Office, is responsible for the implementation, monitoring, maintenance, and evaluation of the *Mobile Device Usage Policy*.

Non-compliance:

Instances or concerns of non-compliance with the *Mobile Device Usage Policy* should be brought to the attention of the Vice-Dean, Education or the Associate Dean, Undergraduate Medical Education, within the College of Medicine.

Procedures:

The Manager, Undergraduate Medical Education, provides overall stewardship to the standard operating procedures associated with the *Mobile Device Usage Policy*.

Contact:

Manager, Undergraduate Medical Education
Phone: 306-966-6142
Email: ugme.medicine@usask.ca