CPSS College of Physicians and Surgeons of Saskatchewan

GUIDELINE

Physician Use of Electronic Communications

Status:	Approved
Approved by Council:	June 2012
Amended:	June 2015 November 2021 September 2023
To be reviewed:	September 2026

PREAMBLE

This document is a guideline of the College of Physicians and Surgeons of Saskatchewan (the "College" or "CPSS") intended for the guidance of Saskatchewan physicians.

Written and verbal communications have traditionally been the primary method for communicating health information between health professionals and patients. Other viable methods have emerged as modes of communication. The use of e-mail has taken on increased significance as a way of clarifying instructions, providing information or to act as a written record.

Although the use of e-mail, text and picture messaging and other internet-based tools for communication purposes has been convenient and inexpensive, it has also created privacy, confidentiality and security issues. Given the vital role physicians play in the protection of their patients' personal health information ("PHI"), physicians must consider the risks associated with the use of electronic communication tools to communicate PHI and take steps to ensure the information is appropriately safeguarded in compliance with Saskatchewan privacy legislation and regulations.

GUIDELINE

1. Purpose and scope of this guideline

This guideline is intended to help physicians understand their legal, professional and ethical obligations when using electronic means of communicating either with patients or with their medical colleagues or other healthcare providers in relation to patient care and management. While the sharing of information can be central to the provision of patient care, the overarching consideration must always be the protection of patients' PHI. In general, physicians who communicate PHI electronically are governed by the same legal, professional and ethical standards that would apply in other professional settings.

While this guideline applies to all forms of electronic communications, it specifically addresses use of the following electronic communication tools:

(a) Telephone

(b) Fax

(c) E-mail

(d) Text and picture messaging

(e) Online video consultation

(f) Social Media

The term "physicians" in this guideline includes all physicians, residents and medical students licensed by the CPSS. In addition to following this guideline, physicians are reminded to be familiar and comply with any other applicable policies and procedures such as those established by the Saskatchewan Health Authority, eHealth Saskatchewan, College of Medicine, or the facility in which they work. In addition, physicians must be familiar and comply with applicable privacy legislation including The Health Information Protection Act (the *"HIPA"*), and should be aware of guidance from the Office of the Saskatchewan Information and Privacy Commissioner (OSIPC).

2. Guiding principles

The following guiding principles are applicable to the use of electronic communication tools by physicians:

- Maintaining confidentiality of patients' PHI is a legal, professional and ethical responsibility of physicians, and is fundamental to the physician-patient relationship.
- Physicians are responsible for the safe and effective management of the PHI of patients in their care.
- While the CPSS recognizes and encourages physicians to capitalize on the advantages available in using electronic communications, they must also be aware of the risks inherent in the use of electronic communication tools[1] with patients or with colleagues in relation to a patient's care and management.
- Physicians who use electronic communication tools remain responsible for the security and confidentiality of the information conveyed as well as the appropriate storage of identifiable patient information.
- Prior to using electronic communication tools to communicate PHI, physicians should consider whether the use of those tools would be secure, appropriate and necessary, and whether the benefits outweigh the risks. Physicians should also consider the appropriate administrative, technical and physical safeguards to protect PHI, as required by the *HIPA* and as discussed in the eCommunication Guidelines published by the OSIPC.
- When communicating electronically with patients, colleagues or other healthcare providers, safeguards should be commensurate with the sensitivity of the PHI and the risks inherent in the electronic communication tools being utilized.
- The patient's consent should be obtained prior to using electronic communication tools other than telephone to communicate PHI to the patient. It is reasonable to expect that patients who use

[1] A major risk in using electronic communication tools to communicate PHI is that the PHI will be inadvertently disclosed to someone who should not have it. This can happen in many ways, including a) unsecure wifi networks, b) emails being sent to the wrong recipient, and c) mobile devices being lost or stolen.

electronic communication tools to solicit PHI from their physicians should be familiar with the risks inherent in using those tools. While written consent to the use of electronic communication tools is ideal, verbal consent may be sufficient. Consent, whether written or verbal, should be documented in the medical record. A sample written consent form is available on the Canadian Medical Protective Association (CMPA) website.

- Physicians are responsible to ensure that the content of electronic communications relevant to a patient's care is recorded in the patient's medical record. In the context of a clinical encounter conducted by telephone or video, the record-keeping expectations are consistent with those for an in-person clinical encounter.

In addition, physicians must take reasonable and appropriate measures to protect the security and confidentiality of their records, including addressing the threats and risk to patient information that is collected, stored or transmitted via electronic means; and to address the security of any mobile devices on which PHI is stored. This includes ensuring appropriate administrative, technical and physical safeguards are in place.

Physicians are encouraged to access the guidance documents of the OSIPC as listed at the end of this document.

3. General guidelines for physicians using electronic communications

(a) Telephone

- There are no guidelines directing physicians to communicate with patients over the telephone. In fact, busy schedules often prevent physicians from phoning patients back during the workday.
- In some instances, a physician may prefer to discuss a medical situation with a patient in person rather than on the phone, in which case their medical assistant should make every effort to book a timely appointment.
- More recently, physicians and patients may choose to have a virtual appointment by telephone, in appropriate circumstances.
- When leaving a telephone or voicemail message for a patient, physicians should exercise caution regarding the content of any message. It is acceptable for messages to contain the name and contact information for the physician or physician's office, but messages should not contain any PHI of the patient such as details of the patient's medical condition or test results.

(b) Fax

- Physicians should adopt a written policy on faxing PHI and ensure that employees, including all new employees, are trained and regularly reminded of the policy. This policy should include the types of information that can be faxed by or to your organization/office.
- If possible, designate one employee to be responsible for sending and receiving PHI by fax. Train that employee in proper procedures and ensure they are aware of the legal duty to protect the information.
- It must be emphasized to anyone faxing PHI that one of the critical steps in preventing a breach is ensuring the correct receiving physician/office is identified before the fax is sent. This requires due diligence given that there are many physicians with the same or similarly spelled or sounding first and/or last names.

(c) **E-mail**

- E-mail is commonly used for communication between physicians and between physicians/patients. Both physicians and patients should be aware of the risks of such a method of communication and agree to assume those risks.
- Physicians should make every effort to ensure that information sent by email is sent from a dedicated professional email account, accessible by an office server in order to access, retain and file any email communications to the patient file; and sent to an email address deemed acceptable by the patient/recipient.
- Physicians should send PHI by email only if it is secured or encrypted or via an attached document that is protected with encryption or password. The password should be supplied by an alternate method, or at least by a separate email.
- Physicians must apply their reasonable judgment in determining whether a patient's consent has been informed depending on the sensitivity of the PHI to be communicated, and should also ensure any PHI is secured or encrypted.
- Physicians should obtain the patient's express consent to using un-encrypted email, after informing them of the limitations and risks of using unencrypted email. It may be appropriate for physicians to use unencrypted email with patients for minor tasks, such as scheduling appointments and appointment reminders, rather than urgent or time-sensitive health issues.
- Consider de-identifying the PHI that will be communicated.
- Ensure recipient contact information is accurate and up-to-date.

(d) **Text and picture messaging**

- Physicians are reminded that text and picture messaging is not typically secure or confidential and therefore should not be recommended as a means of communicating with patients.
- While some texting apps are improving in the level of privacy and encryption offered, physicians must remain cognizant of the risks in using these apps, and to consider those risks when determining the appropriate mode of communication.
- Physicians should determine what type of information can be communicated through text and picture messaging. It may be appropriate for physicians to use text or picture messaging with patients for minor tasks, such as scheduling appointments and appointment reminders, rather than urgent or time-sensitive health issues.
- Physicians should consider whether PHI communicated through text and picture messaging is to be stored on the mobile device and how it will be integrated into the patient's medical record.
- If any photographs or video recordings of a patient are required for providing patient care and/or for documentation, physicians must include a copy of the photograph or recording in the patient's medical record. Once saved to the record, physicians should permanently delete and/or destroy any back-up copy of the photograph and/or video recording.
- Consider de-identifying the PHI that will be communicated.
- Verify the receiver's identity prior to sending PHI.
- Ensure that picture messages do not have any identifiable patient features; use patient initials where possible.
- Ensure that any smart-phone being utilized for patient communication is secured, for example with a 6-digit PIN code and/or Face ID.

(e) **Online video consultation**

- The College recognizes that video consultations are becoming an essential tool in a physician's toolkit, in appropriate circumstances.
- In considering whether a video consultation is appropriate, physicians should refer to the CPSS Policy "Virtual Care."
- Physicians remain responsible for the security of the information and for ensuring the patient has consented to the video consultation.
- Physicians should ensure they are in a private, secure environment to conduct a video consultation, and that patients also have a private, secure area in which to participate.
- Physicians should be aware of the risks involved with various platforms, and are encouraged to consider the information available about the options.

(f) **Social Media**

- For guidance on the use of social media as a communication tool, physicians are encouraged to review the CPSS Guideline "Physician Use of Social Media".
- Physicians must be mindful that there is not only a risk that shared images may be identifiable, but hidden metadata may also reveal identifying data.

4. Seeking advice

If physicians have questions or concerns about the use of electronic communication tools, they may seek advice by contacting the College and asking to speak with a member of the Registrar's staff, or by contacting the Canadian Medical Protective Association for medical-legal advice. The Office of the Saskatchewan Information and Privacy Commissioner may also be able to assist in some circumstances.

Given that the best practices in the area of physician use of electronic communications continue to evolve, physicians are encouraged to stay abreast of current recommendations from the Canadian Medical Association (CMA).

ACKNOWLEDGEMENTS

In developing amendments to this guideline, the College of Physicians and Surgeons of Saskatchewan referenced the College of Physicians and Surgeons of Alberta (CPSA) Advice to the Profession document entitled "Electronic Communications & Security of Mobile Devices", the College of Physicians and Surgeons of Ontario (CPSO) Advice to the Profession document entitled "Protecting Personal Health Information", as well as a number of other resources identified above. The College recognizes, with thanks, the contributions of the CPSA, the CPSO and other organizations to the development of this amended guideline.

OTHER RESOURCES

CPSS bylaws, policies and guidelines:

Regulatory bylaw 7.1 – The Code of Ethics (para. 18, 20)
Regulatory bylaw 7.2 – Code of Conduct ('Confidentiality')
Regulatory bylaw 8.1 – Bylaws Defining Unbecoming, Improper, Unprofessional or Discreditable Conduct (paragraph (x))

Regulatory bylaw 23.1 – Medical Records ((a)(ii) – "in respect of each patient contact")
Regulatory bylaw 23.2 – Privacy Policy

Policy "Ending a Patient-Physician Relationship"
Policy "Establishing a Patient-Physician Relationship"
Policy "Informed Consent and Determining Capacity to Consent"
Policy "Virtual Care"
Guideline "Confidentiality of Patient Information"
Guideline "Physician Use of Social Media"

Office of the Saskatchewan Information and Privacy Commissioner resources or recommendations:

IPC Guide to HIPA
eCommunication: Considerations for trustees to protect personal health information when using eCommunication tools
Helpful Tips: Mobile Device Security
Best Practices for Managing the Use of Personal Email Accounts, Text Messaging and Other Instant Messaging Tools [*intended for public bodies*]
Privacy Impact Assessment: A Guidance Document
Best Practices for Gathering Informed Consent and the Content of Consent Forms
Faxing PI and PHI: Safeguards and responding to a breach
Video Teleconferencing (ITSAP.10.216), Canadian Centre for Cyber Security

Canadian Medical Association resources:

Virtual care playbook for Canadian physicians
Best Practices for Smartphone and Smart-Device Clinical Photo Taking and Sharing
Principles for the Protection of Patient Privacy

Canadian Medical Protective Association resources:

Privacy and confidentiality: Protecting your patient's personal health information (January 2021)
"Top 10 tips for using social media in professional practice" (October 2014; reviewed March 2020)
Virtual care (Updated May 2023)
Texting safely about patient care: Strategies to minimize the risks (June 2019)

Saskatchewan Medical Association resources:

Privacy
Privacy Step-by-Step Guide
EMR Privacy Resources
Virtual Care resources, including Virtual Care – Quick Start Guide