College of Physicians & Surgeons of Alberta

ADVICE TO THE PROFESSION

Telemedicine

Related Standards of Practice: *Continuity of Care, Establishing the Physician-Patient Relationship, Informed Consent, Patient Record Content, Patient Record Retention, Telemedicine*

The College of Physicians & Surgeons of Alberta (CPSA) provides advice to the profession to support physicians in implementing the *CPSA Standards of Practice*. This advice does not define a standard of practice, nor should it be interpreted as legal advice.

Table of Contents

College of Physicians & Surgeons of Alberta

ADVICE TO THE PROFESSION

Background

New digital technologies and growing patient expectations are driving interest in telemedicine as a complement to traditional in-person care. The College recognizes the many benefits of telemedicine: as well as facilitating access to health care for patients, it promises more efficient use of scarce resources, better engagement in personal health, better management of chronic health conditions and easier access to expert opinion. Our role is to enable telemedicine while ensuring patients continue to receive safe, effective care.

This advice document was developed in collaboration with practising physicians, Alberta Health Services, the Alberta Medical Association, and in consultation with the Canadian Medical Protective Association. For additional guidance, refer to the Electronic Communications & Security of Mobile Devices advice document.

Telemedicine Definition

Telemedicine is defined as: "A medical service provided remotely via information and communication technology".[1]

This definition is intentionally broad to acknowledge the rapid pace of technological change. While the tools will change; the principles will remain the same.

Principles

The advice in this document is based on these principles:

1. High-quality patient care is the first priority.
2. The use of telemedicine does not alter the ethical, professional or legal obligations of physicians; regardless of how the physician-patient interaction occurs, physicians **must** comply with the *Code of Ethics*, *CPSA Standards of Practice* and *CPSA Code of Conduct*.
3. Physicians are responsible for determining the appropriateness of telemedicine to support the best outcome for their patient, considering their patients' context and symptoms.
4. Patient privacy and confidentiality of personal health information must be protected.

[1] Reference: Europe Economics. Regulatory Approaches to Telemedicine. 18 May 2018. In this use, the term "remotely" means without physical contact but not necessarily involving long distances.

Registration and Licensing

Physicians with valid registration in Alberta may provide telemedicine services to Alberta patients within the scope of their practice and any conditions on their practice permit. This includes telemedicine services for Albertans temporarily out of the province for work or personal reasons. Non-resident physicians who provide telemedicine services to Albertans only in emergencies do not require Alberta registration.

Alberta physicians providing telemedicine services to patients outside the province should be aware other jurisdictions have their own requirements for medical licensing/registration and liability protection, and the onus is on the physician providing the services to be aware of and meet these requirements.

Continuing Professional Development

Physicians providing telemedicine are expected to maintain competence in the technologies they use for telemedicine services. Related training can be part of the physician's plan to meet mandatory Continuing Professional Development (CPD) requirements. Contact MainPro+ or the Maintenance of Certification Program (as applicable) to determine credit eligibility for specific courses or programs.

The Physician-Patient Relationship

Establishing the Physician-Patient Relationship

A physician-patient relationship is formed whenever a physician gathers clinical information to assess a patient, provides a diagnosis and/or offers medical advice, treatment or support to a patient, including in the telemedicine environment. The ease of digital communications calls for a note of caution: beware of appearing to provide medical advice to non-patients and inadvertently establishing a physician-patient relationship through an online exchange of information. The Canadian Medical Association (CMA) advises physicians can address this risk on an open website by posting a notice describing who the information is for, using a password-protected site and sending a standard, automated response to non-patients.

Just as for an in-person encounter, a physician providing telemedicine care to a patient is expected to perform clinically relevant tasks that may include taking a relevant history, conducting an appropriate examination, requesting diagnostic tests as indicated, referring the patient for consultation as necessary, presenting a diagnosis, explaining the benefits and risks of treatment options, obtaining the patient's informed consent and ensuring appropriate follow-up.

However, telemedicine entails additional responsibilities (listed below) to ensure safe and effective care.

Verify Identity

If there is no pre-existing physician-patient relationship, a physician providing telemedicine must, on first contact with a patient, disclose their name, practice location, registration status and credentials, and be able to produce supporting documentation on request (i.e., practice permit). How this information is disclosed depends on the technology used. For example, it may be posted to the physician's website or in an app, or voiced if using phone or videoconference.

Patients must verify their name, contact information and Personal Health Number (PHN), both for safety reasons and to determine their healthcare jurisdiction for regulatory and billing purposes.

Once a physician-patient relationship has been established, verification of identity may be less formal; however, a higher threshold is appropriate in some circumstances, such as when prescribing drugs associated with substance use disorders or substance-related harm.

Assess Appropriateness

The best interests of the patient must be foremost in any decision about the delivery of care. Telemedicine is appropriate when it will facilitate a good outcome, and may be the best option in some contexts. Telemedicine is also not exclusive to physician-patient interactions; for example, telemedicine between physicians may enable timely consultation about the management of a patient's care.

The value of telemedicine in achieving a quality outcome will differ depending on the circumstances of a clinical case. A quality outcome is defined as safe, timely, effective, efficient, equitable and patient-centred. In determining if telemedicine is appropriate, the following should be considered:

- the patient's presenting condition and clinical history;
- the need for a physical examination;
- time to care (i.e., does it make sense to provide telemedicine immediately, or transfer the patient to care that may be hours or days away);
- patient safety;
- access to other relevant patient information (e.g., pharmaceutical, laboratory, diagnostic imaging or hospital discharge information, etc.);
- other available resources (e.g., technology, support staff, linkages with other healthcare services such as diagnostic laboratory, etc.); and
- relative cost, both for the patient and at a system level.

Where telemedicine is not appropriate, the physician is expected to recommend or arrange an alternative form of care in the patient's best interest (e.g., office visit, referral, emergency room, etc.).

It's important to recognize that the value of telemedicine can change over time in any given clinical situation. An iterative reassessment of the most appropriate mode of care (e.g., telemedicine, home care, in-person care, inpatient care) is essential. For example, if the patient's symptoms continue or worsen, the physician may ask the patient to see them in their office, or direct them to another in-person provider.

Manage Expectations

Physicians providing telemedicine are responsible to ensure their patients understand:

- the care that will be provided by telemedicine and how referrals and continuity of care will be managed;
- how the patient can contact them between encounters, if necessary;
- how quickly they can expect a response to their messages;
- what to do in an emergency situation;
- to whom their health information might be disclosed and for what purpose; and
- fees for any uninsured services.

The physician should also ask for the name of the patient's primary care physician and any other healthcare providers involved in their care for the purpose of ensuring continuity of care (see below).

Obtain Patient Consent

Refer to the *Informed Consent* standard of practice. The same principles apply in telemedicine, and extend to discussing with the patient in plain language:

- the appropriateness and limitations of telemedicine for their care, as noted above;
- the security and privacy risks of the telemedicine technologies being used (email, videoconferencing, apps, etc.);
- measures taken to mitigate those risks; and
- whether encounters will be recorded and recordings maintained in the patient record.

Physicians providing telemedicine are expected to be knowledgeable in the technologies they use and ensure their patients are also well-informed. Conducting a Privacy Impact Assessment will help the physician identify and mitigate security and privacy risks and must be done any time a new technology or procedure is introduced that impacts how patient health information is shared or stored.

To help patients protect their own privacy and optimize their telemedicine experience, physicians should also advise them to:

- use only a secure connection, either a landline or password-protected, preferably encrypted Wifi (public hotspots are not protected and could compromise their privacy);
- check for adequate bandwidth and screen resolution if using videoconferencing technology; and
- find a quiet, private space to avoid interruptions and the potential for others to overhear.

A summary of the discussion and the patient's consent, including explicit consent to communicate sensitive health information using telemedicine technologies, should be maintained in the patient record.

You may wish to direct your patients to the Telemedicine FAQs for Patients on our website.

(Also see Privacy and Confidentiality, below.)

Prescribing Responsibly

As with all prescribing, diligence is required when prescribing for a telemedicine patient: an online questionnaire does not provide sufficient information to issue a prescription.

Physicians must be able to support their prescribing decisions, including documentation of the patient's history and their assessment, other medications the patient is taking and allergies. Physicians also need to employ a high degree of caution when prescribing opioids or other medications associated with substance use disorders or substance-related harm.

Secure transmission of prescriptions is essential to maintain patient safety and reduce the risk of diversion. The most secure method is system-to-system messaging between a secure EMR and the patient's pharmacy; faxing directly to the pharmacy is also acceptable. Prescriptions cannot be provided electronically to the patient for printing.

Refer to the *Prescribing: Administration*, *Prescribing: Drugs Associated with Substance Use Disorders or Substance-Related Harm* and *Cannabis for Medical Purposes* standards of practice and advice documents for further guidance.

When providing telemedicine for out-of-province patients, physicians are expected to comply with jurisdictional requirements pertaining to controlled substances and the authorization of cannabis for medical purposes.

Ensuring Continuity of Care

Telemedicine cannot be provided in isolation, but must be part of a comprehensive approach to care. The obligations for follow-up are the same as for face-to-face encounters. Physicians are responsible for:

When more than one physician is involved in a patient's care, it is important to clarify who is the most responsible physician.

- monitoring their patients and following up any diagnostic tests they order;
- keeping their patient's other relevant healthcare providers informed and providing them with follow-up care information (*Continuity of Care* standard of practice);
- referring their patients as necessary to an acute care facility, an emergency service or another healthcare provider, and providing necessary documentation (see the *Referral Consultation* standard of practice); and
- making appropriate arrangements to stay informed of their patient's progress.

When more than one physician is involved in a patient's care, it is important to clarify who is the most responsible physician. For example, a physician who uses telemedicine to access the advice of a specialist (e.g., telephone consultation) will remain responsible for the patient's care and required follow-up unless the patient is formally referred to the specialist (see *Referral Consultation)* or transferred to another care provider (see *Transfer of Care*).

Any transmission of identifiable patient information must take place in a secure environment (see Privacy and Confidentiality, below).

Recordkeeping

As per the *Patient Record Content* standard of practice, the patient's medical record must include documentation of all patient-related communications, including telemedicine communications in any format (e.g., email, telephone conversation, text message, social media exchange, videoconference, etc.). In general, a summary of the interaction that includes all the relevant clinical information will satisfy recordkeeping requirements.

For example, a physician who consults with a specialist by videoconference is expected to document the patient information provided to the specialist, details of the discussion, the specialist's recommendations, their rationale for accepting or not accepting the specialist's recommendations and next steps. The specialist is expected to document the information received from the treating physician, the substance of their discussion, other information considered in the course of the consultation and recommendations to the treating physician.

As well as supporting continuity of care, the CMPA advises thorough medical records can provide invaluable evidence in the event a question arises about a patient's care. Legal proceedings often start long after consultation is provided, and these records may be physicians' only source of information to refresh their memory or support their testimony.

As outlined in the *Patient Record Retention* standard of practice, records must be maintained a minimum of 10 years (or two years after a minor patient reaches age 18, whichever is longer), and accessible to the patient, other healthcare providers in the patient's circle of care and, with the patient's consent, third parties. For detailed considerations on physician responsibilities related to the security and maintenance of patient records, refer to Physicians as Custodians of Patient Records advice document.

Patient recordings: Physicians should understand patients may also record telemedicine encounters to help them review the physician's advice or instructions at a later time. Under Canadian law, it is legal for individuals to record conversations they are involved in without informing the other party (one-party consent). See Smartphone recordings by patients: Be prepared, it's happening (CMPA)

Privacy and Confidentiality

Physicians must meet or exceed applicable federal and provincial requirements for the privacy and confidentiality of personal health information. In Alberta, physicians are custodians under the *Health Information Act* (*HIA*) and subject to the HIA and its regulations.

Alberta's Office of the Information and Privacy Commissioner (OIPC) advises that patient consent to use electronic transmission does not relieve a custodian of their legal duty to protect the confidentiality of patient information. For detailed guidance and resources, refer to www.oipc.ab.ca

Interjurisdictional communications may also be subject to the federal *Personal Information Protection and Electronic Documents Act (PIPEDA)* and/or provincial or territorial privacy legislation. For more information, contact the privacy commissioners and Colleges in applicable jurisdictions and/or or the CMPA.

Privacy Impact Assessment

Telemedicine is subject to section 64 of the *HIA*, which requires a Privacy Impact Assessment (PIA) of administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information. The PIA must be updated whenever making a change to a practice or system as identified above, including introducing a new tool or technology (e.g., app, software, etc.).

The purpose of the PIA is to demonstrate due diligence in identifying and addressing privacy and security risks as a custodian of patient health information, including:

- foreseeable security risks;
- likelihood of loss/damage;
- seriousness of the potential harm; and
- reasonable (not exhaustive) measures taken to address the risks.

Privacy and security measures for health information must be sufficient and demonstrable to assure the confidentiality of all identifiable patient information, including information transmitted electronically (e.g., prescriptions, diagnostic test requisitions and results, consultation reports and so on). Specific safeguards for prescription transmission are outlined in the *Prescribing: Administration* standard of practice and advice document.

Whenever possible, secure platforms must be used to store and share patient information. When unavailable, take due care to protect the confidentiality of patient information transmitted by email or other electronic means. The OIPC recommends that information transmitted via unsecured networks be encrypted; at a minimum, emails should be password protected. See OIPC Practice Note #5: Communicating with patients via email – know the risks

In some cases, it may be impossible to sufficiently address the risks. For example, web-based platforms that store and

use data for marketing or other purposes unrelated to patient care or health management are inappropriate for telemedicine (e.g., Facebook).

Additional considerations:

- Check the cached data and temporary files in your system: confidential information should not be stored in these areas unless secured or encrypted.
- While email may be secure within the physical confines of a facility, it may not be secure if accessed remotely or wirelessly. Ensure network access is limited to authorized users and/or devices, and that data is encrypted during transmission.
- Transmitted data are often retained and remain accessible on intermediary servers (e.g., service provider, corporate servers) enroute to the intended recipient. Use encryption to protect data from this exposure.
- If telemedicine is provided using a mobile device, there are additional security concerns that must be managed (see the Electronic Communications and Security of Mobile Devices advice document).
- Using a smartphone for clinical photography is convenient and efficient, but safeguards must be in place to protect patient privacy and ensure the security of stored and transmitted images. Refer to Smartphone and Smart Device Clinical Photo Taking & Sharing from the Canadian Medical Association (CMA).
- Patients also have a role in protecting their own privacy, and should be advised to take the basic precautions outlined in Obtain Patient Consent, above.

For detailed information on PIA requirements, go to https://www.oipc.ab.ca/

Use of Social Media

Social media platforms can be used very effectively to share timely, relevant health information with the general public, but are inappropriate for private conversations. The personal/public nature of social media, the rapid and widespread dissemination of information and the blurring of boundaries compel a high degree of caution. Basic precautions include:

- Never provide medical advice to a patient or share confidential information in a non-secure platform.
- Never post identifiable patient information or patient images online (in some cases the nature of the medical condition alone might be enough to identify a patient).
- If a patient or potential patient reaches out to you on social media with personal health concerns, suggest they contact you directly by phone or email to arrange a consultation.
- Use strict privacy settings on your personal social media accounts.

Social media has also become a popular place for the public to freely post opinion on a wide range of topics, including their own medical care. While unverified and rarely supported by evidence, the personal perspectives offered on social media can help physicians identify opportunities to improve the quality of their practice.

For more detailed guidance, refer to the *CPSA Code of Conduct* (applies in all practice settings, including online) and the following:

- Canadian Medical Association: Social Media Policy and Social Media Case Studies
- CMPA: Social networks in healthcare (includes medical crowdsourcing) and related articles

Profiting from Telemedicine Technology Development

Physicians who use, develop or market telemedicine technology products must comply with the *Conflict of Interest*, *Advertising* and *Sale of Products by Physicians* standards of practice.

Duty of Care, Liability and Complaints

Once a physician-patient relationship has been established, the physician has a duty of care. This applies as much in the digital environment as in the physician's office and may extend to consultants involved in the patient's care, even if they have not seen or interacted directly with the patient.

As previously stated, the College expects physicians to provide the same level of care in the digital environment as they would when seeing a patient face-to-face, as outlined in the *Code of Ethics*, *CPSA Standards of Practice* and *CPSA Code of Conduct*.

A physician who does not meet an acceptable standard of care may be subject to the complaints and disciplinary processes of the College. This includes Alberta physicians who provide telemedicine services to patients outside the province, should the College become aware of concerns. While the College cannot investigate complaints from patients within Alberta about out-of-province physicians, the College will provide the complainant with contact information for the applicable regulator.

The CMPA further advises civil action may result from any injury the patient suffers because of that failure. The risk of litigation may be higher in some jurisdictions (e.g., United States), and require additional liability protection. Contact the CMPA for advice.

Resources

CPSA Advice to the Profession

- Electronic Communications and Security of Mobile Devices
- Physicians as Custodians
- Prescribing: Administration
- Telemedicine FAQs for Patients

Canadian Medical Association (CMA)

- Physician Guidelines for Online Communication with Patients
- Smartphone and Smart Device Clinical Photo Taking & Sharing
- Social Media Policy and Case Studies

Canadian Medical Protective Association (CMPA)

- Is that eConsultation or eReferral service right for your medical practice?
- Smartphone recordings by patients: Be prepared, it's happening
- Social networks in health care: Opportunities and challenges for a connected future
- Telemedicine: Opportunities, challenges and obligations
- Videoconferencing consultation: When is it the right choice?
- Thinking of working with virtual clinics? Consider these medical-legal issues

Office of the Information and Privacy Commissioner (OIPC)

- Privacy Impact Assessment
- Communicating with patients via email – know the risks