FAQs on Consent to use Virtual Care

Q. Do I need to collect patient consent to use virtual care for a patient encounter?

CMPA advises in its FAQs on their COVID-19 page (https://www.cmpa-acpm.ca/en/covid19) that patients should consent to the use of virtual care to ensure they understand the benefits, limitations and risks, particularly the privacy risks associated with the technology not present during in-person appointments. Visit the CMA on setting up virtual care https://www.cma.ca/how-set-virtual-care-your-practice.

CMPA states:

> A physician's duty of confidentiality and privacy obligations continue despite the COVID-19 outbreak. Physicians will want to use best efforts to protect their patients' privacy in the provision of virtual care. Physicians should obtain consent from their patient to use virtual care. Such consent should be obtained following an informed consent discussion regarding the increased privacy risks associated with electronic communications and documented in the patient chart, even if it is not possible to obtain a signed consent form from the patient. Patients should also be encouraged to take steps to participate in virtual care encounters in a private setting and through the use of their own personal electronic device/computer.

Q. Do I need to collect consent each time I use virtual care with the same patient.

No, expressed consent, either written or verbal recorded in the patient's record does not need to be repeated at each appointment.

Q. Do I need to collect consent when using Telehealth in the RHAs?

CMPA's advice does not distinguish between type of virtual care tool, the location of the physician or the patient. Currently the RHAs in their use of virtual care rely on implied consent. In the absence of a specific directive from the Government or the CPSNL, the NLMA relies on the advice of CMPA on this matter.

Q. How do I collect consent from patients in long term care?

Whenever possible, consent should be collected from the resident. When a resident is not able to provide consent a physician may rely on the consent provided by the resident or their SDM at the time of admission that gave the RHA consent for the appropriate examinations, investigations, treatments and care. Physicians can also consider CPSNL's Standard of Practice: Telemedicine which states, "Obtain informed consent from the patient, when applicable".

Q. Can someone other than the physician collect the consent from the patient?

Yes, the MOA or someone else working with the physician may collect the consent as long as they are able to record the consent in the patient's record. The MOA can send a consent form to the patient when the appointment is booked and the patient's email is collected. The MOA can also collect and record the verbal consent but the physician should confirm the patient is comfortable using the virtual care tool at the beginning of the appointment.

Q. Is there a recommended text for verbal consent and a form for written consent?

In the Risk Management Toolkit on the CMPA website (https://www.cmpa-acpm.ca/en/advice-publications/risk-management-toolbox) there is sample text for verbal consent and forms for written consent. Sample text for verbal consent:

> "Just like online shopping or email, Virtual Care has some inherent privacy and security risks that your health information may be intercepted or unintentionally disclosed. We want to make sure you understand this before we proceed. In order to improve privacy and confidentiality, you should also take steps to participate in this virtual care encounter in a private setting and should not use an employer's or someone else's computer/device as they may be able to access your information. Please let me know if you want further information on the privacy and security of this call. If it is determined you require a physical exam you may still need to be assessed in person. You should also understand that virtual care is not a substitute for attending the Emergency Department if urgent care is needed. Are you ok to continue?"

The link for the written Consent to Use Virtual Care forms,

- Word doc https://www.cmpa-acpm.ca/static-assets/pdf/advice-and-publications/risk-management-toolbox/com_16_consent_to_use_electronic_communication_form-e.pdf, and
- PDF version https://www.cmpa-acpm.ca/static-assets/pdf/advice-and-publications/risk-management-toolbox/com_16_consent_to_use_electronic_communication_form-e.pdf

What are the Privacy Risks of Virtual Care?

Some of the privacy risks associated with virtual care include: confirming the identity of the patient, others overhearing the discussion by the patient that the physician may not be aware of, and listening into the call by a third party is possible with video consultations if the service the physician is using is not encrypt from end to end or if the patient or the physician is using a public (free) network.

Q. How secure are virtual care tools?

Most companies offering videoconferencing for medical services go through strenuous risk assessments by health organizations before they are approved for use by the organization. When selecting a videoconferencing tool other than those recommended by the Government of Newfoundland and Labrador or eDOCSNL look to see if it has been approved for use in a Canadian province or hospital or is compliant with Canadian privacy legislation.

When using a telephone for a virtual visit a landline phone is generally the most secure. There is a minimal risk of hackers intercepting phone calls when using a cell phone or a handset not attached to the phone.

See Privacy and Security Safeguards in the NLMA Virtual Care Tool Kit.

Q. How do I know if a technology is secure?

Other provinces have conducted privacy and security assessments on a number of tools. The NLMA cannot verify these assessments and doctors must use their own judgement in selecting an application. We suggest contacting the vendor to clarify the following security safeguards:

- Is the transfer of data encrypted? It is recommended that a tool that has end-to-end encryption with 256-bit security certificate as a minimum standard be used.
- What information is collected by the vendor and is it stored outside Canada? Best practice is to choose a tool that uses servers located in Canada as one of the measures to reduce risks.
- Are the videoconferencing sessions recorded? If a tool does have the ability to record, we recommend disabling this feature – ask your vendor for support.
- Is there phone support or just email? What hours is it available?

Q. How do I ensure that the device I am using for virtual care is secure?

All systems, applications, and devices used for virtual care should be behind a firewall with anti-malware and anti-virus software installed. These are services you should have installed on both your office and home computers, laptops, tablets and phones. You should ensure the device used for videoconferencing is not obsolete and software is current so the most recent updates can be applied. Furthermore, all devices should be password protected using a complex password.

Q. How can we ensure we are talking to the right patient?

Just as with an in-person visit, the MCP number can be used to identify the patient. You can also ask to see picture identification. You should also ask the patient to confirm that they are the only person who can hear their conversation or if there is another person in the room are they comfortable with that person being there. If you cannot confirm the identity of the patient or senses the patient is uncomfortable with the other people that can hear the conversation an in-person appointment should be arranged.

Q. Is it ok for patients to send documents by email?

Physicians should discourage patients from sending any personal health information, including photographs by email or text.

Resources related to Consent for Virtual Care

- CMPA COVID-19 Information, https://www.cmpa-acpm.ca/en/covid19
- CMPA Risk Management Toolkit, https://www.cmpa-acpm.ca/en/advice-publications/risk-management-toolbox
- NLMA Virtual Care Toolkit, http://www.nlma.nl.ca/FileManager/VirtualCare/docs/2020.03.22_NLMA_Virtual_Care_Toolkit.pdf