

Guidelines for consent for virtual health visits

Introduction

This Patient and Care Team Digital Communication Policy provides advice for your use of Digital Communications both as part of the COVID-19 response and beyond. It has been reviewed and approved by the Information Privacy and Security Standing Committee, the Chief Information Officers Digital Leadership Committee, the Office of the Information and Privacy Commission and BC Health Regulators. Each Health Authority had privacy and security leads involved in the policy development.

This policy was a collaborative effort amongst provincial health colleges and the health authority privacy and security leads and the Ministry of Health. Work began on the policy prior to our COVID-19 response, with plans in place to work with policy offices, practice leads, health authority legal teams and clinical programs to implement, educate clinicians and staff, and to review any needs for existing policy and guideline changes.

Due to COVID-19 the policy was expedited on the approval of the Office of Information and Privacy Commission and the Digital Leadership committee, and the tool was quickly provided as part of the virtual health toolkit for immediate guidance. We highly recommend you discuss with your program leadership who can help put this new information in context with your current practice.

In the meantime, it is hoped that this direction will enable you to best meet your patients' needs to receive care and be healthy at home. Please use it in the context of your organization and program needs. If you have questions, please contact provincialvirtualhealth@phsa.ca.

The policy describes how staff and health care providers can use the following digital health communications:

- email
- phone
- text
- video chat
- other types of electronic transmission of patient information

It is intended to guide policies and practices, along with organization-specific requirements.

Obtaining patient consent

Step 1

Introduce Virtual Health to patients and notify them of the risks

Provide the [Patient Notification for Digital Communications](#) form to the patient, and/or verbally review the content with them. Documentation is not required as the policy **does not rely on written consent**, but is confirmed through the patient identify validation process. See the suggested script for the initial conversation at the end of this document.

Reference: Appendix A of the Patient and Care Team Digital Communication Policy (see page 13).

Step 2

Validate patient identity prior to sending any personal information

Ask the patient to contact the provider directly by sending a communication to the provider by email, text or through an application. This confirms the patient's identity and reduces the risk of unauthorized disclosure of personal information. It also establishes a "digital relationship" that can continue as long as the patient continues to receive information and reply to digital communication.

Options for validating include:

- Provide your contact information and ask the patient to send the first message
- Send an initial text or email to confirm you have connected with the right person
- Ask the patient to verify by text or phone to provide information only they would know, such as last 4 digits of PHN, date of last clinic visit, month/year of birth or other previously agreed upon information.

Reference: Appendix B of the Patient and Care Team Digital Communication Policy (validation script, see page 14).

Step 3

Communication

Having followed steps 1 and 2, you are now ready to provide digital communications to patients for:

- Patient care
- Scheduling appointments
- Providing results
- Providing follow up instructions

Not Permitted

Medication prescribing is not permitted in digital communications. SRFax and TurboScan are endorsed solutions for submitting electronic prescriptions, and information on both can be found in the COVID-19 virtual health toolkit. This is not considered digital prescribing.

Large/bulk data requests must be encrypted according to organization policy.

Digital Communications are prohibited in emergencies (unless no other option exists or there is no other means of contacting).

Other information

- Communication between members of the care team does not require consent by the patient but unnecessary personal information should be excluded.
- If there is a significant lapse in time from the last digital communication with a patient, identify validation as describe above should be repeated.
- Digital communications with a patient's family, friends or representatives should only occur if the patient has consented to the disclosure of information or the disclosure is authorized by legislation.

Reference: Page 6 of the Patient and Care Team Digital Communication Policy.

- For health authority care providers and staff, employer-provided devices and applications approved by the organization must be used, and if personal devices are used, this must be appropriate and consistent with the organizations direction on the solution being used. If personal devices are used, reasonable security measures must be used.

Reference: Appendix C Patient and Care Team Digital Communication Policy (see page 15).

- Restrict information on what is relevant and necessary for the purpose of the communications, based on the "need to know."
- Emails and texts are considered transitory communication, and there is no legal requirement to keep them. Refer to your program and organization protocols.

From Step 1: Example of a short privacy/consent statement you may want to use with your patient/client

"To begin, I'd like to confirm that you received the [Notification of Risk document](#) that was sent to your email. If you haven't received it, I can send it again right away.

We'll do what we can to confirm that any personal information we send is being received by you and only you, by asking for verification of your identify.

We want to make sure you understand this before we proceed. In order to protect your privacy and confidentiality, please participate in this virtual health visit in a private setting, and do not use an employer's or someone else's computer/device as they may be able to access your information.

Are you okay to continue? Do you have any questions?"