

Electronic Communications with Clients

August 2020

Background

With the increasing ubiquity of smartphones and convenience of corresponding by email and text, clients are indicating a preference to communicate with health care providers this way. ACOT has been fielding an increasing number of inquiries from OTs requesting guidance on communicating with clients electronically.

The convenience of, and often your client's preference for, communicating electronically must be balanced with your legislated obligation to ensure the security and retention of those communications.

This guideline has been prepared based on the advice of ACOT's legal counsel as well as the recommended practices outlined by the Office of the Information and Privacy Commissioner (OIPC). This guideline also aligns with the directives provided by Alberta Health Services (AHS) and many other employers of OTs in the province that are required to adhere to the *Health Information Act* (HIA), the *Freedom of Information and Protection of Privacy Act* (FOIP) and/or the *Personal Information Protection Act* (PIPA).

Applicability of these Guidelines

This guideline has been prepared for OTs who are self-employed/operate their own business, and/or whose employers/contractors do not have policies and procedures in place regarding electronic communications with clients. It is intended to support OTs in maintaining the security of client records as per applicable information privacy legislation and Code of Ethics indicator 1.6 which requires OTs to *"safeguard client information from unwarranted disclosure."*

If your employer does provide guidance on electronic communications but it does not meet or exceed the guidance provided below, follow ACOT's guidance.

ACOT Guidance

1. Informed consent to communicate via email/text must be sought and documented for each client/guardian.
 - Even if a client/guardian consents to use of electronic communications, this does not absolve you of your responsibility for the security of these communications.
 - Any breaches of a client's health or personal information must be reported to the Office of the Information and Privacy Commissioner (OIPC). Breach reporting forms and resources can be accessed from the OIPC's [How to Report a Privacy Breach](#) page.
2. Secure, encrypted devices and email/text applications should be used.
 - Best practice is to keep the client/guardian's phone number separate from their name on your phone. This can be done by leaving the phone number as is in your contacts or to use some form of coding system.

- A “test” email/text message should be sent prior to sending any other information to verify that the message is being sent to the intended recipient.
- 3. Communication via *text* should be restricted to appointment confirmations and request for call backs.
- 4. Communication via encrypted *emails* can include links or attachments to appropriate resources for clients/guardians or password protected documents if secure communication portals are not available.
 - Identifying information within the content of the email body should also be limited whenever possible (e.g. use generic subject lines, avoid use of identifying descriptions/pronouns, do not include health or other personal information of any type).
 - The encryption key or password should be sent separately (e.g. via voice message).
 - Avoid sending to a client/guardian’s workplace email; use a personal account (note: if a client/guardian’s email address has their last name in it – that is already one piece of identifying information).
- 5. Communication via email or text is considered a part of a client’s record and thus plans should be in place to store and retain these communications securely for the required time period.
 - The time period client records are to be retained can vary based on the information privacy/record retention legislation applicable to your employer/contracting organization or your area of private practice.
 - ACOT’s guidance is to retain records for *at least 11 years and three (3) months after the last date of service provided or 11 years and three (3) months after your client turns 18 if they were a minor when services were delivered.*¹

Additional Resources

- AHS has created a guide on the risks associated with email communication and how to mitigate those risks - [User Guide for emailing personal health information](#).
- The Office of the Information and Privacy Commissioner (OIPC) has prepared an advisory on [Communicating with Patients Electronically](#).
- The OIPC has also prepared a guide on the considerations for using personal devices versus employer provided/approved electronic devices - [Privacy and Security risks of a “Bring your Own Device” program](#).

¹ ACOT has updated the guidance on record retention based on recent legal advice. It reflects the requirements of the *Limitations Act* which was amended in 2017. Refer to the **Standards for Documentation** practice guideline for an explanation of this retention period.