**CDA INTERIM GUIDANCE**

**PATIENT PRIVACY AND THE USE OF TELEDENTISTRY COMMUNICATION TOOLS
DURING COVID-19 PANDEMIC**

The Canadian Dental Association has prepared these guiding principles to assist you in supporting emergency care to patients in need when in-office visits are not possible. Unlike other healthcare providers such as physicians, dentists may have had less experience using such tools. Note that teledentistry is dentistry, and your professional obligations with regard to all regulations and expectations are unchanged when providing virtual care.

During the pandemic, in-office patient visits are restricted to “emergency care” only. Some Colleges have provided the criteria for a patient “emergency” on their websites; in other cases, such advice is not available and decisions are left to the judgment of individual dentists. The use of virtual care tools at this time is to enable you to make the best possible assessment without an in-office examination of a patient’s complaint to determine how the patient’s condition should be managed. Many Colleges are continuously updating their guidance on the practice of dentistry in the face of COVID-19; it is prudent to review their guidance on a regular basis.

Use the following four general principles to guide patient interactions when an in-person visit is not possible. These do not replace or supersede guidance provided by your regulatory College. The principles are:

1. Understand the Privacy Risks of Virtual Care Tools
2. Obtain Informed Patient Consent
3. Ensure Record Keeping Meets Regulatory Requirements
4. Exercise Your Professional Judgement

Each principle is discussed below, followed by some practical tips for using electronic communication tools with patients.

**PRINCIPLE #1: Understand the Privacy Risks of Virtual Care Tools**

There is an increasing number of electronic communication tools available to the public to facilitate distance communications such as email, text messaging and videoconferencing.

***However, these consumer-based tools may not meet your professional regulatory and legal obligations to maintain the privacy of your patients, and the confidentiality and security of their health information. Mobile devices pose particular risks if unencrypted health information is stored on a device that is subsequently lost or stolen. Further, the terms and conditions of “secure” online services may compromise patient privacy by including things such as the right of the service provider to “scrape” information from your communications. Note as well that many electronic communication tools are available in different versions, one for consumers and others for use in specific sectors, such as health and education. Those designed for a specific sector generally state the sectoral privacy legislation with which they are compliant.***

***Such consumer tools may not be appropriate to use to deliver virtual care to patients. Non-public facing remote communication products that provide health system-level privacy and security compliance should be the “tool of choice”, and encrypted applications preferred over unencrypted applications. Your regulatory College may have specific requirements as well.***

The term “unregulated” is used to describe those virtual communications platforms that are not specifically designed to be used by the healthcare sector. A list of common, **unregulated, virtual communication platforms** includes:

* Skype and Teams by Microsoft
* Facetime by Apple
* Zoom Basic
* Google Hangouts
* WhatsApp by Facebook
* Doxy.me
* Texting
* Regular email

A phone call is a good starting point for a teledentistry encounter. If you receive a text or email, ask the patient for their phone number and call them—perhaps a voice conversation is all that is needed to assess the patient. At that time, if you feel that the communications method used by the patient is not secure you can suggest another more secure, privacy protective mechanism.

Dentists who have subscribed to the CDA Secure Send service can use the service to send information such as messages, documents and images, including sensitive patient information, to anyone, including patients, in a secure manner that is compliant with provincial and federal privacy laws, as well as the requirements of the dental regulatory Colleges. However, CDA Secure Send does not enable two-way communication between a dentist and a patient; only dentists subscribed to the service can use CDA Secure Send to reply to message.

If a video conference is needed, or images need to be exchanged, decide with the patient the most effective communication method that also best mitigates risks to patient privacy and confidentiality and security of their health information.

**PRINCIPLE #2: Obtain Informed Patient Consent**

Obtaining patient consent is a mechanism to protect yourself from the privacy challenges of modern electronic communications. You cannot provide a guarantee to a patient that their health information contained in any electronic communication will remain secure and confidential. Your patients must clearly understand the risks involved in communicating with you using such communications to receive virtual care. So whenever possible, before using virtual care tools, you should obtain the express, informed consent of the patient to communicate with them in this manner. Ideally this is written consent and you should insist on getting this consent prior to engaging in the electronic communication. If it is not possible for you to obtain the express, written consent of the patient prior to engaging in the electronic communication, you should, at the earliest opportunity, explain the risks to the patient and document their consent in the patient record.

These are the steps you should take:

1. **New Patients**

If you are dealing with a new patient, you should first confirm the identity of the patient and provide the patient with proof of your identity, as well as your licensure status.

You may advise the patient:

“As a professional practicing dentist, I am obliged to let you know that my name is Dr. **[provide your full name]**. I am licensed to practice in the province of **[insert province]** by **[insert name of College]**; my College licence number is **[insert number]**.

1. **Explain the Risks to the Patient**

You may use the following statement to explain the risks to the patient prior to the first use of virtual care tools:

“Virtual Care has some inherent privacy and security risks that your health information may be intercepted or unintentionally disclosed. I 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 or device as they may be able to access your information. Are you ok to continue?”

1. **Confirm the Patient’s Consent to the Use of Electronic Communications**

After receiving a verbal confirmation as suggested above, you should provide the patient with a fuller explanation of the privacy and security concerns and receive an explicit “I agree” from the patient. For example, you could email the following information:

“As you are aware, COVID-19 is placing extreme stress on Canada’s public health system. Our office is offering emergency virtual care to make sure that we can provide such care for our patients safely and effectively. This means that we will be using electronic communications for emergency patient visits who require it when our office is closed. Some of these technologies are provided by vendors such as Google, or Apple to help make discussions with your dentist as easy as possible when a dental emergency arises. Some dental emergencies may be addressed with virtual care alone, but in some cases your dentist may ask you to visit an emergency dental clinic for a physical examination.

We do our best to make sure that any information you give to us during virtual care visits is private and secure, but no electronic communications tools (such as audio, video, email, text) are ever completely secure. There is an increased security risk that your health information may be intercepted or disclosed to third parties when using such electronic communications tools. You should also understand that we will assume no liability in the event that your health information is the subject of a privacy breach. You may have a claim against the provider of the electronic communications tool.

To help us keep your information safe and secure, you should:

* Understand that electronic communications (such as audio, video, email, text) you receive are not secure in the same way as a private appointment in an exam room.
* Use a private computer/device (i.e., not an employer’s or third party’s computer/device), secure accounts, and a secure internet connection. For example, using a personal and encrypted email account is more secure than an unencrypted email account, and your access to the Internet on your home network will generally be more secure than an open guest Wi-Fi connection, such as that available in a public place.

You should also understand that virtual care is not always a substitute for in-person communication or clinical examinations, where appropriate, or for going to an Emergency Dental Clinic when needed (including for any urgent care that may be required).

If you are concerned about using electronic communications for virtual care, you can ask our office to attempt to arrange a potential alternative. However, please note that visiting a health care provider in person comes with a higher risk of coming into contact with COVID-19 and the possibility of spreading the virus.

By replying to this message with an “I agree”, you agree to let us collect, use, or disclose your personal health information through video, audio, email, or text communications to provide you with care. In particular, the following means of electronic communication may be used such as audio, video (including Skype, Facetime, etc.), email, text, etc.].”

As shown in the last paragraph, request that the patient confirm their consent by responding to the communication with a simple affirmative statement such as “I agree”.

1. **Document the Consent in the Patient’s Record**

A statement such as the one below may be used to document the patient’s consent, either before or during the virtual care visit in the patient record.

“Informed consent was obtained from this patient to communicate and provide emergency care using virtual care electronic communications tools. The risks related to unauthorized disclosure or interception of personal health information and steps they can take to help protect their information have been explained to the patient.”

It is anticipated that during this period of the COVID-19 pandemic, email and/or text messaging may be the most common form of electronic communications, besides the telephone, used by dentists to communicate with their patients requiring emergency treatment.

**PRINCIPLE #3: Ensure Record Keeping Meets Regulatory Requirements**

All patient communication using virtual care tools such as email, text and videoconferencing must be recorded according to the professional regulatory requirements for the maintenance of patient records. Consult your provincial regulatory body for advice on what information exchanged with a patient using electronic communications must be incorporated into the patient record to satisfy your professional record-keeping obligations.

**PRINCIPLE #4: Exercise Your Professional Judgment**

As practicing healthcare professionals, dentists are in the best position to decide what patient conditions can be managed using virtual care tools and the tools that can best support the virtual visit to manage the COVID-19 public health crisis while respecting all applicable regulatory requirements.

**PRACTICAL TIPS FOR USING ELECTRONIC COMMUNICATION WITH PATIENTS**

Remember that obtaining patient consent is the key risk management process for dentists providing emergency teledentistry care to your patients. Patients do, and will communicate with you using any tool with which they are familiar and use on a regular basis to communicate with their friends and family. Once you have explained the risks to them and obtained their consent, you and your patient may use such tools for teledentistry.

You do not need to, nor should you, provide patients with advice on which electronic tools should be used for teledentistry: the adequacy of the privacy, confidentiality and security controls of such tools to exchange health information continues to shift, with experts disagreeing on which satisfy the legislative and regulatory requirements of healthcare professionals.

Nevertheless, here are some practical tips that will assist when using various types of electronic communications with your patients.

**Phone**

If you have forwarded your office phone to your personal phone (mobile or land line) and using your personal number to speak with patients:

* Block your phone number so that it does not appear if the patient has Caller ID
* Use the regular calling features offered by your telecom provider as opposed to applications for making calls to avoid unknown use, access, recording of calls by such applications

**Text**

* Do not use any social media platforms
* The use of instant messaging applications is also extremely problematic because of the use that may be made of the contents of your communication with your patients

**Email**

* For sending messages, use CDA Secure Send. It is available to dentist members of the CDA Corporate Members, and individual CDA members in Quebec. It is free, secure and you can send a message to any email address ([sign in here to subscribe](https://services.cda-adc.ca)). However, only registered users (dentists) can reply.
* One option for receiving messages from a patient, is to have the patient send you a password-protected PDF, and call you to provide the password. See below for examples on how to password-protect a PDF.
* Always ensure that you confirm that you are using the correct email address prior to communicating with a patient and that you include “Personal and Confidential” in the description of the message

 **Video Conferencing**

* The tool of choice should be a service dedicated to healthcare
* Use consumer-based services only if you judge that a video conference with a patient is necessary and these are the only available option
* Do not use any social media platforms

**Receiving Files**

* Remember that email attachments are not secured by default; password-protected PDFs are an option.

**Sending Files**

* Use CDA Secure Send to send to patients or other dentists.

**Image and File Retention**

* Any patient health information that is retained on a mobile device must be encrypted to avoid a privacy breach if the device is lost or stolen
* The best practice is to transfer all communications content, text and images from your mobile device into the patient record as soon as the teledentistry session is completed and delete the information from your device

**Use of Mobile Devices – Mobile Phones and Laptops**

* The device of choice should be the one you use for your dental practice
* If you do use your personal device to communicate electronically with patients, there are numerous steps that you should take to ensure that these communications are private, confidential and secure.
* These steps include the following:
	+ Only use your professional email address
	+ Ensure that no one else, such as family members, has access to or uses your device
	+ Check that you are using secure WIFI (i.e. one that requires a password)
	+ Maintain constant backed-ups of the information on the device
	+ Do not leave your device unattended – keep it in a locked room or drawer

**Use Microsoft Word to create a password-protected PDF**

1. Paste any images or content into a Word document.
2. Choose File > Save As.
3. Under Save as Type, choose PDF (\*.pdf)
4. In the Save As dialog box:
	1. Provide a File name
	2. Choose Tools > General Options (located near the Save button)
5. In the General Options dialog box, enter a strong password in the “Password to open” field.
Select OK.
6. Select Save in the Save As dialog box.
7. The pdf document created will now require the password to open it.