Guidelines for using telehealth in dentistry during the COVID-19 alert level response

17 April 2020

Dental Council
Te Kaunihera Tiaki Niho

Introduction

Purpose

The purpose of this document is to provide guidelines for registered oral health practitioners when using telehealth during the period when the COVID-19 alert levels (1-4) apply.

Context

Telehealth is the term for the use of information and communication technologies to deliver healthcare when clients and care providers are not in the same physical location. (NZ Telehealth Forum 2015).

During the COVID-19 alert response, there will be times when you can provide only urgent or emergency care for patients. This is in an effort to reduce community spread of COVID-19, including to yourself, your staff and your patients.

This will require you to triage a patient by phone first and decide whether they require urgent or emergency care, or whether care can be deferred.

A range of information and communication technologies can be used when using telehealth. This could include phone or videoconference calls, emails, telehealth applications, fax; or shared information folders to submit, store or transfer health information.

Guidelines

General

- Understand that as soon as you interact with a patient using telehealth you are providing care.
- Be aware of the inherent risks in providing care using telehealth when an assessment and diagnosis of the patient's condition cannot be made in person[1]. Ensure you do not provide care which puts the patient's health or safety at risk.
- If in your professional judgement the patient needs a face-to-face assessment to make an accurate diagnosis, or needs treatment to effectively manage their urgent/emergency dental condition, then do so if you can meet the respective alert level's room and PPE requirements. If you are unable to meet these requirements or the patient requires care you cannot provide for any other reason, refer the patient to where they can receive the care they need.
- Be conscious that the Council's Standards framework for oral health practitioners and the Code of Health and Disability Consumers' Rights applies to all forms of care delivery, including telehealth.
- Remember your obligations related to the Informed consent and Patient records and the privacy of health information practice standards.
- Use technology that will allow you to gather the information needed to enable you to make an accurate assessment and diagnosis of the patient's condition, to inform your plan for further care. For example, a video call and digital photo may provide greater information than a phone call in some circumstances.

[1] When the patient and practitioner are physically present in the same room.

During consultation

- Protect the privacy and confidentiality of the patient's health information by:
    - doing the telehealth consultation in a private environment that will ensure the patient's private information will not be overheard or seen by other individuals in your vicinity
    - confirming with the patient that they are in a private setting where they can give honest and accurate answers to questions relating to their care.
- Early in the telehealth consultation, confirm the identity of the patient, especially if it is a new patient. Also inform the patient of your scope of practice and confirm that you hold a current annual practising certificate. If relevant, disclose any conditions or limitations on your scope of practice.
- Obtain consent from the patient, parent, guardian, or carer to proceed with the consultation.
    - Do not video or voice record patients without their consent when collecting their health information, and provide information regarding the intended use of the video or recording as part of that consent process.
    - Get permission if you are going to access other health data systems to obtain further information on the patient's health record, such as for prescribing purposes; or if the consultation record will also be stored in another provider's health system (for example in a DHB's Titanium in addition to your practice patient record system).
- Advise the patient upfront of any consultation fee and available payment methods.
- Obtain a complete medical history that includes:
    - screening questions for COVID-19 infection contained in the Council's Guidelines for oral health services at the different COVID-19 Alert Levels.
    - past medical history
    - current conditions
    - current medication (prescribed and non-prescribed)
    - allergies.
- Obtain a history of the patient's dental condition and confirm the nature of the emergency/urgent care before recommending next steps, which may include:
    - advice and prescription of appropriate medication, if indicated
    - asking the patient to come into the practice/clinic for an assessment and/or treatment
    - facilitating referral of the patient when you are unable to provide the required care safely and competently; and within your scope of practice.
- Obtain informed consent from the patient, parent, guardian or carer for the care you plan to provide.
    - Given the unfamiliar environment within which these consultations may occur, encourage your patients to ask questions and give them the opportunity to discuss with you the various options for care, and their preferences and concerns.

- Make sure the patient understands the information you have given them. Check whether your patient needs any additional support to understand the information, communicate their wishes, or to make a choice; and assist in arranging this, as needed and available.

- If over-the-counter or prescription medication is required:
    - prescriptions can be sent to the pharmacy for collection without the patient presenting at the practice/clinic
    - where prescriptions are issued to suspected or COVID-positive patients, please ask the patient not to attend the pharmacy themselves to pick it up – they should send a family member or arrange delivery by the pharmacy (delivery may incur a cost)
    - follow the new rules for electronic prescriptions to support virtual care in the community, published 2 April
    - follow-up with the patient that the medication prescribed has resolved the issue.

Patient records

- Ensure that you keep an accurate and complete record of the care you are providing during this time.
- If you cannot remotely update your patient records immediately following the consultation, make sure you retain the patient information and your notes, and add these to their patient record as soon as possible to ensure you maintain patient records that are comprehensive, time-bound and up-to-date.
- Record all the information typically needed for your patient record.

Privacy and security of health information

- You must ensure security safeguards are in place to protect your patient's health information.
- Do not leave patient notes unsecured, either physically or on an electronic device.
- Delete the information from any personal device as soon as it has been transferred into the patient record.
- The Council's Patient records and privacy of health information practice standard contains specific advice on how to protect the security of your patients' health information. An excerpt of this advice is included as Appendix 1 for ease of reference.
- We acknowledge that during this unprecedented time, and with limited time to prepare for a lock-down scenario, some of the mechanisms may not be in place or fully operational at this time. However, it remains your professional responsibility to protect the privacy and security of the patient health information you hold.

Acknowledgements

These guidelines are founded on a number of sources including the Medical Council of New Zealand's *Telehealth* (2020); the Nurse Executives of New Zealand position statement *Telehealth* (2015); the Australian Dental Association's policy statement *Dental informatics and digital health* (2019); the American Dental Association *Policy on teledentistry* (2015); the Pharmacy Council's *Statement on telehealth and supply of pharmacy services over the internet* (2019); and the Ministry of Health's *Information sharing advice for health care workers* (2020).

Excerpt on health information security measures from the Dental Council Patient records and privacy of health information practice standard

Security of health information

7 You must ensure security safeguards are in place to protect patient health information.

Guidance [1]

Physical security

➢ Protect the physical security of patient information by:

- Physically securing and restricting access to the areas in which patient information is stored. Take simple precautions such as locking filing cabinets and locking unattended rooms.
- Requiring password access to computer systems where patient information is stored, and using access lockout after a fixed number of incorrect login attempts.
- Positioning computer screens so that they cannot be seen by unauthorised persons.
- Using security screen saver programmes to prevent unauthorised persons from seeing computer screens and having automatic log-off of computer systems after a set period of non-use.
- Protecting patient records from physical hazards, for example, fire.
- Backing-up patient records regularly, and testing recovery of information from the back-up.
- Storing records that are not being used for current or regular patient care, but that need to be legally held, in a manner that protects their security.

Operational security (Users)

➢ Protect the security of patient information by:

- Keeping patient information confidential—disclose health information only to the patient, or their representative, unless an exception applies (see standard 13).

[1] Standard 7 corresponds to Rule 5 of the HIPC

- Not accessing the health information of patients you have not provided care for, unless an exception for the use or disclosure of health information applies (see standards 10 and 13)
- Ensuring team members understand their obligations in relation to the confidentiality and privacy of patient information.
- This includes an understanding that patients' health information cannot be discussed with anyone other than team members who already hold this information, unless an exception applies. Where practical, any discussion involving patient information should occur in private areas of the practice, not in shared spaces such as the waiting room, reception area, or staff room.
- Avoiding collecting patient information verbally in public waiting areas, where discussions can be overheard
- Keeping patient information on the premises where possible, and keeping information secure when there is a need for it to be off-site, for example, storing 'archived' patient records off-site.
- Anonymising patient information when being used for health education purposes, and using fictitious information when training individuals in the use of systems.
- Withholding, as far as practical, access to patient information from IT services personnel.

Operational security (Computer systems)

➢ Protect the security of patient information by:

- Maintaining a list of team members who are authorised to use the system.
- Managing authorised users' access consistent with their role, so that access to patient information is on a 'need-to-know' basis.
- Using strong passwords and changing them at regular intervals.
- Making sure that computer access leaves a footprint that is regularly audited to detect unauthorised access.
- Providing training for team members on the proper use of the computer system, which includes how the security and privacy of patient information is protected.

Technical security (Computer systems)

➢ When selecting and maintaining a computer system for the collection of patient information:

- Use only software designed for recording, processing, storing and retrieving patient information.
- Set up security, firewalls, and anti-malware systems to protect patient information from direct unauthorised access, and unauthorised access through hacking or invasion of hostile or intrusive software.
- Use a back-up system which allows information to be stored remotely from the main computer system, preferably off-site.

➢ If you are using remote servers hosted on the internet to manage and/or store patient information (also termed 'cloud computing'), you remain responsible for the security of that information.

The same applies if you are using a third party for storage of patient information in digital form where the remote server is not internet based.

Make sure that when using these services patient information is sent and stored safely by being assured:

- that the data is automatically encrypted when it is being sent between your practice and the remote server
- of the physical and digital security of the remote sever.

The Privacy Commissioner's *Cloud Computing A guide to making the right choices* provides further detailed guidance in this area.

Security of transmission

➢ Consider developing a practice procedure for sending out patient health information that reflects the guidance below:

For email	• Consider the nature of the information to be sent, who the intended recipient is, and whether email is the most appropriate form of communication. If the email recipient is a patient, confirm that you have their permission to communicate with them in this way. • When sending sensitive information, encrypt email contents (both user and recipient will need to use the same encryption), or use password protection. • Ensure email addresses are accurate and current. • Consider using a secure email service. • Do not use lengthy 'chains' of responses in emails, as sensitive information may be unwittingly included by an earlier response. • Limit the number of "cc" addresses to only those who must receive the information.
For post	• Ensure the type of physical delivery is appropriate for the nature of the information (general post, registered post, couriered post, track-and-trace, and hand delivered post). • Ensure addresses are accurate and current. • Ensure postal items are kept secure until lodged.
For text messaging	• Check you have the patient's consent to send them text messages, for example, appointment reminders; and record their consent or refusal in the patient record. • Do not include clinical information in text messages.
For facsimile (Fax)	• Limit the use of fax machines to authorised persons and control the type of information that may be sent. • Programme fax machines with frequently called numbers to reduce the risk of misdialing (regularly check the accuracy of these). • Check that correct transmission has occurred, and respond rapidly in the case of incorrect transmission.

➢ Do not give patient records to third parties, such as the patient's relatives or friends, to hand deliver to a patient, unless authorised by the patient concerned, or the person is the patient's representative.

Security during destruction

- Destroy physical records by controlled incineration or shredding, ensuring that no information is lost or removed during the process and that the resulting waste does not include fragments of readable personal information. Alternatively a reputable document destruction company can be used.

- Destroy computerised records by using an appropriate electronic or physical process to ensure the record is unreadable. Simple deletion from the device may be inadequate as data recovery is possible. Seek expert advice if you are unsure.

Security breaches

- Act promptly to manage an actual or suspected breach of patient information. Appendix B outlines key steps that could be followed, and be incorporated into a practice procedure which specifies how to deal with information breaches.