

Telepractice — Telehealth

Telepractice, or telehealth, by a dietitian is the provision of professional dietetic services over short or long distances by telephone, facsimile, e-mail, internet connection and/or video conferencing systems to a client/patient. The technology used in telepractice leads to some special considerations in dealing with the security of records and consent to treatment. Many dietitians in Ontario have asked the College for assistance. The College is responding by providing the following guidance.

In providing telepractice service, dietitians are asked to consider the fundamental principles of good record keeping by referring to Chapter 6 of the *Jurisprudence Handbook for Dietitians in Ontario* and the *Standards of Practice* (www.cdo.on.ca > *Resource Room* > *Professional Practice*). Chapter 4 and 5 of the *Handbook* deal with Confidentiality and Consent to Treatment.

The following chart starts with the specific principles and goes on to provide guidance particular to telepractice technologies. The College requests feedback on this guidance and asks that you let us know of any additional telepractice issues you may face. The College is prepared to explore developing further support for dietitians who provide telepractice dietetic services. Contact us through www.cdo.on.ca or email gignacm@cdo.on.ca or phone the Registrar, Mary Lou Gignac, 416-598-1725 or 1-800-668-4990.

You may also wish to view the work of a national interdisciplinary group who developed a framework of guidelines for telehealth. The *National Initiative for Telehealth* (NIFTE) report is available at www.nifte.ca

Also for legal requirements relating to personal information see:

Government of Ontario Home>Canada NewsWire-Ontario Newsroom

www.ontla.on.ca>*Bills* (go to Bill 31)

www.cdo.on.ca>*Resource Room*>*Legislation* (PIPEDA)

Guidance on the Confidentiality and Security of Records used in Telepractice

General Principles:

- Telepractice communication with a client constitutes a dietitian-client relationship in the same way that any face to face encounter would constitute a dietitian-client relationship. The integrity and the value of this relationship should be maintained and should not be diminished by the use of telepractice technology.
- The content and nature of the communication, and not the format or length of the communication, should determine the need for documentation and what is recorded. Significant telecommunications are documented in the same way that significant face-to-face communications are documented. The manner in which they are documented may vary according to the technology used.
- The same professional obligations that exist for consent, confidentiality, and security of information in face-to-face dietetic services also exists for dietetic telepractice services.

The technologies themselves and the use of the technologies will affect what dietitians should do to ensure confidentiality and security of records.

The following table provides guidance to RDs on how these principles may be applied in dietetic telepractice:

Principles	Guidance About the Application of the Principles
<p>Consent</p> <p>Informed consent must be obtained in accordance with the <i>Health Care Consent Act</i> and the CDO published guidelines. Informed consent must be obtained where it cannot be reasonably implied.</p>	<ul style="list-style-type: none"> • To ensure informed consent, clients should be provided with information about service as well as how the technology will be used in delivering the service. This would include information about who is assisting with the delivery of the service and thereby have access to the client's information, e.g. a technician operating equipment, a supervisor monitoring for quality assurance, or a consultant providing assistance with an assessment or treatment plan. This would also include any information about how information is transmitted and any risks associated confidentiality, e.g. the risks associated with email information that is not encrypted. • Clients should always provide consent for any taping of a conversation and be provided with information about how the tape will be used and how it will be stored (e.g. where, for what period, who has access to it). • Where the service involves multiple sites and/or facilities, it must be made clear in policy and protocols who has the responsibility to obtain and record the consent where it is not implied.
<p>Keeping Records</p> <p>All the College's regulations, standards and guidelines relating to members' conduct and practice apply equally to telepractice and face-to-face services.</p>	<ul style="list-style-type: none"> • Dietitians providing dietetic services using telepractice technologies must follow the record keeping provisions in the CDO Proposed Regulation "Records Relating to Members' Practice" available in the Resource Room at www.cdo.on.ca><i>Proposed Regulations</i>. Record keeping is also discussed in the new <i>Jurisprudence Handbook for Dietitians in Ontario</i>. As such, the information recorded should include findings from the assessment, recommendations and treatments, and communication with other health care providers. • It is advisable that the charting include information about the type of communication (e.g. telephone, email, video conference) and the format of assessment information (e.g. whether anthropometric measurements were verbally provided, in written or electronic image format, or directly measured. Forms may be developed for efficient charting of such information. • "Received" and "sent" emails should be filed in the client chart and phone conversations charted if they contain material relevant to a client assessment and nutrition intervention.
<p>Access to Records</p> <ul style="list-style-type: none"> • Records must be retained for 10 years following a client encounter or 10 years following the 18th birthday of the client, whichever is longer; • Clients have a right of access to their health records, and; • Records may be reviewed in a College investigation, Quality Assurance process or for a legal proceeding including an investigation made pursuant to a search warrant. 	<ul style="list-style-type: none"> • Records must be maintained in a format that ensures retrieval. They may be retained in electronic format – however, where there are electronic records as well as hard copy ones, they should be linked to ensure a complete record is made accessible as required. • Where records exist in electronic format, there should be attention given to the capacity to retrieve and print the record throughout the full retention period, even as systems and software changes are made. • Dietitians should ensure that electronic records are reliably backed up. This is as important to the independent practitioner as it is to large facilities. Hard drives can "crash" affecting access to records, and computers are targets for theft including the information on hard drives. • Where there are multiple sites and practitioners, issues of ownership of records should be dealt with in policy to ensure proper custody of records for the full retention period.
<p>Confidentiality and Security of Records</p> <p>Dietetic services delivered through telepractice are subject to the same principles of client confidentiality as are all other types of dietetic care.</p> <p>Dietitians in telepractice are accountable for the security, confidentiality and access to records.</p>	<ul style="list-style-type: none"> • RDs in telepractice should understand the security risks of all the information technologies they use and do what is necessary to manage all risks related to potential breach of confidentiality. All reasonable steps must be taken to ensure that the technology and protocols used in telepractice and its documentation are designed to protect against loss, tampering, interference or unauthorized use or access. • For instance, emails are not considered to be secure. Emails can be intercepted or inadvertently delivered to the wrong address, even if sent within a single location. Hard drives can "crash" affecting access to records. Computers are targets for theft including the information on hard drives. • Password systems, encryption and proper back up systems are as important to the independent practitioner as it is to large facilities. • Telepractice services are advised to develop confidentiality and security protocols in consultation with experts in the field of information technology. • RDs should also familiarize themselves with the confidentiality policies and protocols of their employer and be aware of the risks in order to protect themselves and convey them as necessary to clients in seeking informed consent.