Privacy considerations with telehealth consultations – Who owns your telehealth medical information? How is it being used and disclosed?

Date: 26 June 2020

Abstract: One of the impacts of the social distancing restrictions due to the COVID-19 pandemic, has been the rise in the usage of telehealth technology. This technology has enabled patients to receive general medical consultations in a safe environment whilst maintaining social distancing.

A regular visit to your local GP involves filling out a brief medical history and a few lifestyle questions regarding your health, on your initial visit. This may be followed by a face-to-face consult with your doctor. However, the advent of telehealth technology meant that the initial consult requires a patient's personal information to be communicated in an online form and the follow-up consult conducted over a phone call phone call, video conference or messaging/chat functions.

This change in format for 'attending' an appointment with your health professional leads to many questions about the ownership of the data provided in these telehealth conferences and how it can be collected, used and disclosed. Your personal medical history and current medical concerns are considered to be 'sensitive information' and 'health information' under the *Privacy Act 1988* ('the Privacy Act') and afforded protections against its collection, use and disclosure under the 13 Australian Privacy Principles (APPs) in Schedule 1 to the Privacy Act.

Who owns your medical records in general?

In a regular face-to-face visit, your doctor takes notes to compile information about your health in order to facilitate treatment. Generally, it is the doctor or the doctor's surgery who owns and maintains the health record (*Breen v Williams* (1996) 186 CLR 71).

While as an individual you may not own the medical records, if the doctor's surgery is an APP entity, you are be able to access your own health information (such as medical records) pursuant to APP 12.

There are ten grounds on which the doctor's surgery as an APP entity can refuse to give access. These are:

- that the surgery reasonably believes that access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety;
- giving access would have an unreasonable impact on the privacy of other individuals;
- the request for access is frivolous or vexatious;
- the information relates to existing or anticipated legal proceedings between the doctor and the patient, and would not be accessible by the process of discovery in those proceedings;
- giving access would reveal the surgery's intentions in relation to negotiations with the patient in such a way as to prejudice those negotiations;
- giving access would be unlawful;
- denying access is required or authorised by or under an Australian law or a court/tribunal order;

- the surgery has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to their functions or activities has been, is being or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter;
- giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body;
- giving access would reveal evaluative information generated within the doctor's organisation in connection with a commercially sensitive decision-making process.

Using or Disclosing Medical Information

Doctor's surgeries can use or disclose medical information about a patient for the primary purpose for which it was collected under APP 6. For example, if a patient provides a doctor with their health information during a consultation, the primary purpose of the doctor collecting their information is to provide general practice services to diagnose and treat that patient.

Doctors can use or disclose medical information about a patient for a secondary purpose in certain circumstances such as:

- with the patient's express consent;
- it is reasonably expected and the purpose is directly related to the primary purpose of collection, such as a medical referral;
- required or authorised by law;
- it is unreasonable or impracticable to obtain consent and there is a belief that the use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety;
- to conducting research, or to compile or analyse statistics; and
- to preventing a serious threat to the life, health or safety of a genetic relative.

Who owns your Telehealth records?

While there are privacy matters relating to the ownership and use of medical information, the added inclusion of telehealth technology adds further complexity to the situation. As the telehealth technology used by a doctor may not be owned by the doctor's surgery, there could be issues regarding the ownership and usage of the medical information, the chat technology, identifiers or the recorded footage, where applicable.

Unless the telehealth technology is developed and owned by the doctor or their surgery, the ownership of the data acquired in a telehealth appointment may be derived from the agreement the doctor's surgery has with the third-party provider.

How can your Telehealth records be used and disclosed?

The concerns regarding the ownership of a patient's telehealth medical records also extends to its use and disclosure. As per APP 7, an organisation can only use or disclose a patient's health information for direct marketing, being the direct promotion of goods or services to an individual, if the patient has provided consent. A patient's health information includes their name and contact details.

Companies have been accused of data selling and platform misuse, when they provided data to Medicare and other third parties as part of their payment platforms in an attempt to assist the doctors they were partnering with. While some of these disclosures can be considered unintended

consequences that were rectified in a fast- evolving situation, the greatest concerns relate to organisation that pass on an individual's private medical information to other organisations such as personal injury law firms and private health insurance brokers.

While users may not think they have consented to this secondary use of their medical information, it may be perceived that the ticking of the box next to the privacy policies/terms and conditions prior to a telehealth conference grants consent, even if the individual did not read it.

In August 2019, the Australian Competition and Consumer Commission ('ACCC') brought a lawsuit against HealthEngine for selling the information of 135,000 patients, including their name, phone number, email address, date or year of birth, between April 30, 2014 and June 30, 2018 to private health insurance brokers. The ACCC argues that HealthEngine HealthEngine used language whish suggested that HealthEngine itself provided the health insurance services and did not adequately disclose that the patient's personal information would be sent to one of the Insurance Brokers or that HealthEngine would receive a payment for doing so. The proceedings are ongoing.

The rise of the use of telehealth technologies have enabled many to obtain a medical consult within the privacy of their home. However, the sudden shift from face-to-face consults to telehealth consults during the COVID-19 pandemic, has meant that the ownership of the medical information accumulated during these appointments may not be clear. Therefore, it is important that the health professionals who utilise this technology have the appropriate agreements in place with their telehealth providers to ensure that they or the patient retain the ownership of the patient's medical information and that it does not get used and disclosed by the telehealth technology company without the patient's consent.