Privacy and security in connected hearing healthcare

BY BILL CAMPBELL

The COVID-19 pandemic has forced audiology services across the globe to find new ways of working. This has resulted in a rapid increase in the uptake of remote care and, with it, some new privacy and security considerations.

Connected hearing healthcare

The concept of remote connection between clinicians and patients for the purpose of providing components of hearing healthcare has been around since at least 2000 [1]. With the ongoing development of technology, and particularly with the onset of the global COVID-19 pandemic, recent interest in connected hearing healthcare has grown significantly. Connection to patients may be as simple as a discussion regarding hearing aid maintenance to something as complex as the hearing assessment of an infant using auditory brainstem response testing. All major hearing aid manufacturers now offer proprietary remote connections to a patient's hearing aids via mobile apps and websites [2]. Connections to patients can range from a simple telephone conversation to a complex connection involving audio/video and data transfer over a Wi-Fi network.

The issue

The importance of patient privacy and data security in clinician/patient interactions cannot be overstated. Legislation and regulations governing patient confidentiality varies from country to country and within regions, and can be quite complex. The hearing healthcare provider must be aware of all relevant legislation, professional regulations and guidelines, as well as agency policy and procedure. Although clinicians must have a working understanding of the rules governing their particular practice, a complete understanding of the legislation is a challenge, even for legal professionals.

Privacy legislation is a body of legal literature that has evolved over time. As new technology emerges, new regulations are patched on to existing documentation, creating a legal tangle that is beyond most clinician's ability to interpret and integrate into practice. In this regard, there is a significant need for regulatory guidance for clinicians.

"New regulations are patched on to existing documentation, creating a legal tangle that is beyond most clinician's ability to interpret and integrate into practice"

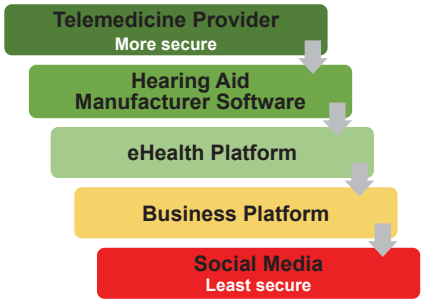
The risks

Can a remote session be compromised? Under certain circumstances, a video conference and/or data transfer session can be intercepted and viewed [3] . If security at the hub (the site where the clinician is located) or the spoke site (where the patient is located) is poor, a session can be overheard, or information can be obtained that would facilitate unwanted access.

What does third party usage mean? At first glance, the issue of data security seems simple. Data is transferred using a software solution and is then stored by the clinician in a patient file, electronic or otherwise. However, clinicians must understand

that any data transmitted using an online product or solution does not necessarily travel exclusively from point to point. Video data is often stored by the software solution host, and may be accessed for a variety of reasons, including sharing with third parties for marketing and development purposes. Data (including video/audio data) that is transmitted online may be stored on servers in locations outside of the country or region in which the clinician is practising, and this may violate privacy legislation.

The solutions



Know the relevant legislation in your practice. This depends on the country, state, province, and region in which you are practising. Consider government legislation as well as guidelines and policy dictated by professional bodies and the clinic's agency. It is the clinician's responsibility to operate under the relevant rules. Clinicians should seek help from their professional regulatory bodies (where available) in understanding the complex regulatory environment.

Use common sense. If it doesn't feel secure, it probably isn't. This holds true for the hub and spoke environments as well as for the solutions used for the remote connection and data storage. Just as you wouldn't share sensitive personal information over social media, interacting with a patient over social media is inappropriate. This includes non-secure video chat platforms such as Skype (excluding Skype for Business), Facebook, FaceTime, etc. Many videoconference solutions offer free versions of their platform. However, privacy safeguards may vary with product levels, so be sure that you are using an appropriate option. The privacy statements of any app or solution provider are often complex, however it is important to understand key aspects such as encryption level, server locations, third party data access and so on.

Deidentify. Keeping a record of remote sessions stored without any patient information is key in preventing compromise of that patient's personal or health information. Wherever possible, use only a unique identifier that can be code-referenced to the patient's hard copy or secure electronic medical record. This is of particular importance in instances where data is entered and stored on a device located at a hub site. Avoiding the logging of any identifying patient information ensures that privacy cannot be compromised if the device is stolen or accessed.

"Clinicians must understand that any data transmitted using an online product or solution does not necessarily travel exclusively from point to point"

Ask for help. There are several trustworthy resources who share the responsibility of patient data security. Your professional regulatory body or college has a responsibility to protect the public and, as such, has current knowledge of relevant legislation. Developers of software solutions can provide information regarding the security of their product. Hearing aid manufacturers with remote options built into their software share a significant part of the responsibility for data security and can assist in appropriate use of their solutions.

Who is responsible?

When the clinician is the sole custodian of patient information, the issue of protecting information is less complex than it might be in a large agency or hospital setting. "In a traditional clinical setting, where the information is collected by the practitioner, the responsibility for maintaining personal health information falls squarely on the clinician" [2]. It is the clinician's responsibility, among other things, to obtain informed consent from the patient. The clinician should endeavour to avoid all possible risks, however mitigating every risk is not possible. The patient must understand these risks before consenting to services. When the clinician is sharing or storing, intentionally or inadvertently, information with other parties (agency intranet, third party software supplier), those parties must share the responsibility for protecting client information. Whether it be a hearing aid manufacturer's app or a web-based videoconference solution, the developers of the solution must take steps to ensure data is secure.

The role of the hearing healthcare provider is first to ensure that their own practices are in keeping with relevant privacy legislation, regulations, and guidelines. The clinician must then assure themselves that their own organisation, whether it be a small clinic or a component of a larger agency, has taken steps to ensure that networks and devices are secure [4]. Additionally, it is the clinician's responsibility to establish to the best of their abilities that the solution in use meets relevant privacy legislation. The clinician must take it in good faith that the solution is as secure as it claims to be and must keep their knowledge current [2]. A solution's privacy policies may change over time and that may impact the compliance with relevant legislation.

"Everyone must keep in mind that if the patient is not safe – or does not feel secure – then there will be bigger problems than cleaning up a data breach or dealing with a compliance audit. You'll be facing a crisis of confidence by the very patients that telemedicine is designed to help" [3].

References

1. Givens G, Blanarovich A, Murphy T, et al. Internet-based tele-audiometry System for the Assessment of Hearing: A Pilot Study. *Telemedicine Journal and e-Health* 2003;**9(4)**:375-8.
2. Campbell W, Shelley J, Jiwani S, et al. Remote connectivity technology: Privacy considerations for eAudiology applications. *Canadian Audiologist* 2020;**7(3)**.
3. Blanco AG. Video calls and security; Is it true my webcam can be hacked? BBVA. May 2020. www.bbva.com/en/video-calls-and-security-is-it-true-my-webcam-can-be-hacked/
4. Utter J. Telemedicine is Surging, but What About Security?. Security Roundtable.org. May 2020. www.securityroundtable.org/telemedicine-is-surging-but-what-about-security/

Both links last accessed November 2020.

AUTHOR

Bill Campbell, MClSc,

Audiologist (retired), Ontario, Canada.