Canadian Audiologist

The Official Publication of the Canadian Academy of Audiology

Remote Connectivity Technology: Privacy Considerations for eAudiology Applications

Published May 4th, 2020

Bill Campbell, MClSc, Reg CASLPO
Jacob Shelley, LLM, SJD
Salima Jiwani, PhD, MSc, Reg. CASLPO
Robin O'Hagan, BA
Danielle Glista, PhD, Reg CASLPO

Recent advancements in connectivity technologies have enabled the clinical reality of remote service delivery across many health professions. Remote service provision in audiology has helped facilitate access to care and reduce direct/indirect service costs.[1] The current COVID-19 pandemic has disrupted face-to-face care in audiology due to social/physical distancing regulations but has offered a shift in focus towards remote service delivery models to allow for continued patient accessibility. Telemedicine efforts have been a part of our society since the 1960s. Within audiology, the first documented audiological test via the internet dates back to 2000,[2] indicating that remote audiology delivery has been around in some form for several decades.

The terminology used to refer to remote service provision within the field of audiology has been ever-evolving; tele-audiology, telepractice in audiology, and eAudiology are all terms used to describe the use of information and communication technologies to remotely connect the patient to audiological services. eAudiology is defined as encompassing technologies and services that enable remote provision of audiologic care at each stage along the patient journey, including screening, assessment, coaching, adjustments, monitoring, assistance, rehabilitation, and aftercare.[3] eAudiology is not meant to replace traditional face-to-face, in-person care, but rather, to complement it. It is a timely growth for the virtual care model that considers technological innovation and accessibility that is wide-reaching.

Audiologists are now taking a fresh look at incorporating remote connectivity options into their practices using technologies that can access, process, and store health information. This has led to a plethora of questions and concerns, as audiologists wade into unfamiliar territory. Specifically, the potential risks and limitations of electronically mediated interactions are of concern to many. The obligation to protect patient privacy by ensuring information security is a responsibility that needs

to be upheld during eAudiology appointments. Figure 1 illustrates the components of maintaining patient privacy, as it relates to legislative influence, in addition to the foundations of security: confidentiality, access, control, and integrity[4]. Although the opportunities presented via connectivity technologies are great, not all technologies are the same when it comes to ensuring privacy. eAudiology services can be delivered in many ways, from telephone conversations to video conferencing to remote connections to hearing aids, with each application offering its own set of privacy and confidentiality concerns. This article will speak to current challenges audiologists are facing when choosing a secure tool/technology to deliver remote services to patients and will guide audiologists as they look to integrate technologies and ethical considerations of remote services into their practice.

Privacy in Practice

Privacy concerns should always be at the forefront of any health care practice. Concerns about breaches in privacy are limited when both the clinician and patient's environment is secure; this is easier to ensure when using face-to-face, in-person mediated interaction. With the use of alternative modalities on the rise, so too are concerns about privacy. Technological advances to deliver services to patients can take a variety of forms. For example, technology-mediated communication between an audiologist and patient can occur with the use of video conferencing, allowing an exchange of information at a distance with both audio and visual cues. Videoconferencing can support lipreading and instruction-based communication, but also requires access and patient familiarity with technology. Another common eAudiology application includes the use of remote hearing aid support tools. The ability to remotely connect to a patient's hearing aid is now possible via platforms supported by every major hearing aid manufacturer. The plethora of support tools being offered to achieve

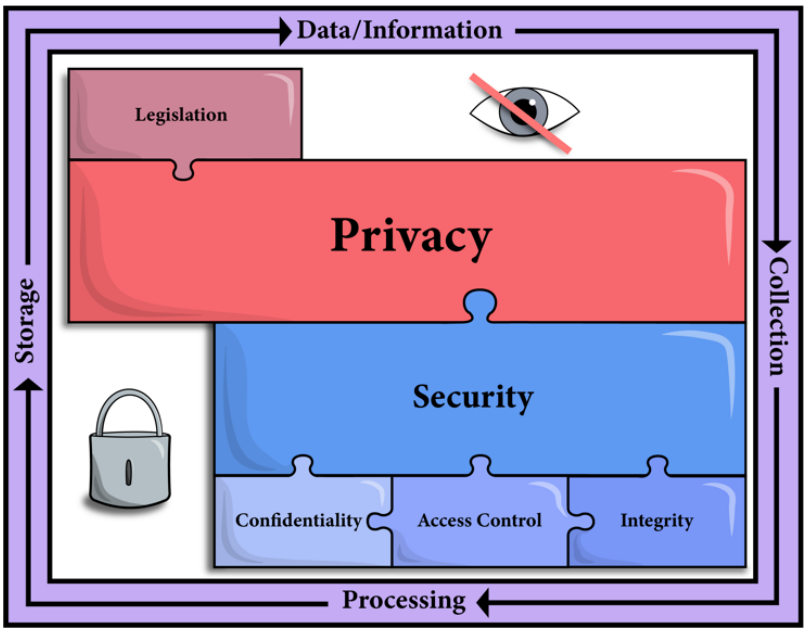

Figure 1. Illustration of the pieces of the puzzle that need come together when considering the privacy and security of technology-mediated service delivery.

eAudiology are both exciting and overwhelming, with a dizzying array of potential video conferencing and data sharing solutions available.

Audiologists may not be well-equipped with the knowledge to adequately understand and interpret the legal quagmire around privacy legislation considerations and health information governance unique to technology-mediated data/information exchanges. Furthermore, the information provided on this topic can be confusing and highly complex. While all health care providers should educate themselves on the technology they seek to use in practice, including assessing whether it adheres to legislative requirements, vetting all service platforms is unrealistic. Rather, a great deal of the onus for ensuring privacy arguably lies with the developer of the connectivity technology in question. Developers must ensure that their product or solution is compliant with privacy legislation that is relevant to the region in which it will be sold and ultimately used. Moreover, regulatory bodies and colleges also share a significant degree of responsibility, including ensuring that audiologists not only have access to guidance documents around the clinical practice considerations related to remote service delivery but also, that they are adequately assisted with navigating the terms of privacy when using the recommended connectivity technologies for eAudiology.

> At a minimum, it is not the responsibility of the health care provider alone, instead, a coordinated effort across the profession is required; this involves the active engagement of specialty and professional organizations related to the field of practice as well as those in information technologies, to put into place appropriate education and support for practicing clinicians.[5]

While it is not reasonable to expect that individual audiologists will be equipped to assess and integrate all of the intricate details of health care legislation when using each eAudiology tool, it is necessary for every clinician to have a basic understanding of privacy legislation and how it applies to eAudiology applications. Such knowledge will help each audiologist recognize their fundamental responsibilities in the context of remote service provision.

Privacy Legislation in the Context of Technology-Mediated Health Care

Privacy legislation in Canada can rightly be called a quagmire. It exists as a patchwork of legislation, common law, and equitable principles. There are multiple, overlapping statutes, that might govern an individual in a situation for a variety of reasons. At the federal level, there are two laws governing privacy: The Personal Information Protection and Electronic Documents Act (PIPEDA)[6] and the Privacy Act.[7] PIPEDA governs the collection, use, and disclosure of personal information during commercial activities (s. 4(1)(a)), while the Privacy Act applies to the collection, use, and disclosure of personal information by the government. For both acts, personal information refers to identifiable information about an individual, such as their age, race, or medical history.[8]

Clinics providing health care are subject to PIPEDA, with some provincial exceptions. If the government is satisfied that provincial legislation is “substantially similar” to PIPEDA, it may exempt organizations in the province from complying with PIPEDA (s. 26(2)). In such instances, organizations engaged in commercial activities must instead adhere to the substantially similar provincial legislation. This is the case in several provinces, including Ontario, at least for health

care providers, as the Personal Health Information Protection Act (PHIPA)[9] has been found to meet this requirement.[10] In Ontario, PHIPA sets out the rules about the control and custody of personal health information by health information custodians, which for present purposes, includes audiologists. Consequently, audiologists must ensure that their management of the personal health information of their patients, is compliant with PHIPA. In provinces that do not have legislation that has been deemed substantially similar, practitioners may have to adhere to different governing rules.

Complicating matters further are international norms. For example, the General Data Protection Regulation[11] (GDPR) in the European Union and the Health Insurance Portability and Accountability Act[12] (HIPAA) Privacy Rule[13] in the United States. Many technological platforms that practitioners may rely on will not be situated for use in Canada and may only identify themselves as compliant with GDPR or HIPAA. Indeed, many platforms available to audiologists are located elsewhere and are often advertised as GDPR or HIPAA compliant. As of yet, there is no recognition that either the GDPR or HIPAA are substantially similar to PIPEDA, and thus it is not enough for a clinician to rely on GDPR- or HIPAA-compliance as a safeguard.

While there will be jurisdictional variation in the rules set out how audiologists must protect patient information, the onus is on practitioners to ensure that patient information is protected. For example, health information custodians in Ontario are required, among other things, to:

- Obtain consent for the collection, use, and disclosure of health information;
- Take steps to safeguard against theft, loss or unauthorized collection; and,
- Inform both patients and the provincial privacy commissioner of any privacy breaches or unauthorized uses.

> In a traditional clinical setting, where the information is collected by and maintained by the practitioner, the responsibility for maintaining personal health information falls squarely on the clinician.

It is less clear, however, in practices employing new technologies, what the specific responsibilities and liabilities are for clinicians who maintain less control over the information.

In response to this uncertainty – and, of late, due to the demands for clarity imposed by shifts in practice owing to COVID-19 – some governments have been trying to guide practitioners about the uses of new technologies. For example, the Provincial Health Services Authority (PHSA) in British Columbia released a COVID-19 Virtual Health Toolkit that identifies technologies that the Ministry of Health and PHSA endorse “for immediate use under the emergency response due to COVID-19.”[14] The Toolkit provides a comprehensive overview of the various tools a practitioner can employ to connect with a patient. Nevertheless, guidance such as this does not go far enough to ensure clinicians using innovative technologies in their practice that does more than simply connect a practitioner with their patient, are compliant with privacy legislation.

As the delivery of online health care services increases, and not just in response to a pandemic, but as a way to ensure that patients in remote or underserved areas can get access to care or to assist patients that might not be able to attend a health care appointment in person. Privacy laws and expectations of individual clinicians must evolve accordingly.

> Perhaps COVID-19 will force regulators to contend more comprehensively with the burgeoning use of new technologies in health care and the implications on privacy,

> the relationship clinicians have with patients, and the liability that clinicians may face.

Until such a time, all clinicians should, at a minimum, ensure that the technologies they employ are compliant with privacy expectations and do their utmost to safeguard patient privacy.

All Tools and Technologies are NOT Equal

In the absence of clear, definitive guidelines on the use of technology by audiologists for the delivery of remote care, we propose an approach to gauging where a technology fits within a ‘hierarchy of privacy.' Critically, despite our proposed approach, if an audiologist opts to use technology in practice to connect with patients, that clinicians should satisfy themselves that the platform they are using is sufficiently secure to meet applicable legislation and minimize any possible harm to their patient. However, we propose that the degree of responsibility that lies on the audiologist themselves will vary depending upon the solution that they are using and on the guidance that they have been given (about that solution specifically or more general guidance).

Where a platform provider appears to have taken more responsibility in developing a solution, such as in the case of a telemedicine software platform or a commercial eHealth platform, this may shift some of the onus of responsibility to the clinician. The platform delivering services via such solutions is subject to PIPEDA or the substantially similar provincial legislation, and thus, ought to take measures to ensure their platform is compliant. In situations where clinicians have been given specific regulatory guidelines or information about how to adhere to statutory requirements, as is the case in the example of British Columbia’s Virtual Health Toolkit, this may lift the onus of responsibility off of the clinician and place it back on the regulatory body. Thus, an audiologist may consider that there is a ***‘hierarchy of privacy,’*** which can act as a guide to determining what platforms are appropriate for videoconferencing and data sharing. Generally, eAudiology solutions that are single purpose, and that bear a significant amount of privacy risk place a greater amount of responsibility on the platform provider to ensure privacy. This section will discuss how a privacy hierarchy can be applied to some of the popular eAudiology tools and discussion around what to look for when assessing levels of privacy and security (Figure 2).

Figure 2. illustrated some key factors to consider when assessing where a tool fits into the privacy and security hierarchy.

Traditional Telemedicine Platforms

These can be considered a more secure option when researching solutions. Telemedicine emerged as a solution dedicated to the remote provision of health care in Canada. These platforms carry a significant burden of risk and, as such, presumably have taken steps to ensure compliance with all applicable privacy regulations and policy. Although multidisciplinary, telemedicine platforms are often single-purpose and specialized; they have the additional benefit of built-in, real-time technical support. Each province and territory in Canada has at least one telemedicine platform provider. In some territories, the service is provided by an adjacent province, such as Nunavut, which shares services with Alberta. Telemedicine networks, however, may not be a viable solution for many practices. The ability to access a telemedicine network for audiology may vary, as many clinics operate as a for-profit entity and may not fit the criteria for inclusion in a telemedicine network. Publicly funded not-for-profit clinics or programs (such as early hearing detection and intervention programs) may be able to utilize telemedicine networks more readily. Access and fee structures may be dependent on the status of the audiology clinic. Additionally, fees for use of provincial telemedicine providers can be significant as well.

Remote Hearing Aid Support Tools (Manufacturer Specific)

These options can be considered to have a higher degree of security as they have been developed to GDPR compliance – although as noted above, compliance with GDPR should not be considered failsafe. As the major hearing aid manufacturers all have an international presence, most (if not all) recognize the need to be compliant with all jurisdictional legislation and have developed their software solutions accordingly. These options are easily accessed via platforms like HIMSA's Noah 4 or through stand-alone hearing aid software modules provided by manufacturers. To understand the implications for privacy, it is helpful for audiologists to have a full understanding of the remote options available in a manufacturer's software platform and their various uses. Privacy agreement notices are offered by each manufacturer, offering important details for clinicians. These applications are not meant solely for hearing aid programming adjustments and may be used for coaching, rehabilitation sessions, or general technical assistance, for example.

> It is important for patients to be fully informed of the various applications and how

these applications will collect, use, and store information.

Commercial eHealth Solutions

These often come with adequate security features, when compared to solutions that are not specific to healthcare solutions, but care should nevertheless be taken to ensure that the solution chosen meets the privacy regulations and expectations of your jurisdiction and your regulatory bodies. Like telemedicine platforms, commercial eHealth platforms are often single purposed and multidisciplinary, with a focus on video conferencing capabilities. eHealth solutions, such as Zoom for Healthcare, generally, will comply with privacy legislation/certification – this information is readily available in privacy statements accompanying such solutions. As eHealth becomes a global enterprise, more software developers are recognizing the risks involved and the need for meeting international privacy standards. Commercial eHealth solutions generally involve subscription costs and can offer a variety of features aimed at improving scheduling, record keeping, etc. Audiologists should evaluate the needs of their clinic and their patients when choosing an option.

Business Adapted Solutions

These solutions, often focusing on virtual meetings, including platforms such as Skype for Business, Zoom (general purpose), Cisco WebEx, as a few examples. As they are designed to meet the needs of businesses, they may not consider the requirements governing the confidentiality of health information. While the encryption of data and the overall security of the connection may be enough for a consultation with a patient, the details of that connection may be stored on a third-party server in an unsecured manner. Specific feature categories of interest in these platforms include the ability to record session data. While these features may be useful for some purposes, they nonetheless require that the recorded session is ultimately stored at a different location. This storage site may be accessible to other parties for purposes that a patient may not have consented to, such as marketing or aggregate data analysis. Many platform providers offer a "free" version of their product. Audiologists should ensure that the free versions carry the same compliance and security as the paid version of the product. In many cases, the paid version simply allows access to more features, like scheduling or multiple attendees. However, with some solutions, the free versions may be less secure, with the paid version offering password-protected sessions and better encryption.

Social Media Directed Solutions

At the lowest end of the hierarchy of privacy are videoconferencing and data sharing solutions designed for social interaction and general public use (e.g., FaceTime, Google Groups, and Facebook Video Chat). These platforms should be considered vulnerable and should not be used for clinician-to-patient connections. While many patients may use social media rather freely – and perhaps even suggest it as an appropriate way to connect – there are serious privacy concerns that arise through this use. For example, connecting to a patient through social media may violate the patient’s privacy and confidentiality, as this potentially public connection is an indication that they are receiving some sort of hearing health care. In instances where patients initiate contact through social media, it is the clinician’s responsibility to immediately direct communication to a secure means.

Considering the Ethical And Appropriate Use of Technology

Beyond the solutions mentioned above, there is a wide variety of commercial solutions available to enable eAudiology and they are evolving at a rapid rate. Most offer varying tiers or categories of fee structures that may be associated with different levels of privacy. Feature differences can help differentiate whether a specific platform may be appropriate for the eAudiology application of

interest. Feature information can also highlight security ‘add-ons’, such as password protection and encryption, that assist in the maintenance of privacy.

Ultimately, ethical practice in eHealth and eAudiology should drive technology choice. In addition to privacy and security considerations, an ethical practice involving connectivity technology should also be considered[5]:

- Patients interests and needs;
- Clinician competency/technology skill level and ability to provide a high level of care;
- Transparent and informed consent processes;
- Continuity of care; and,
- Understanding of the limitations of eAudiology care.

It is clear, particularly in the current circumstance of the COVID-19 global pandemic, that the use of technology in the delivery of care is on the rise. As patient/clinician needs change, so too will the technology adapt to meet these needs. Clinicians and clinics will not be static in their use of technology, but instead, will adapt and evolve as the technology does. In light of this, it would be impractical to suggest a particular technological platform for use in practice. Instead, a checklist is provided below to help guide audiologists in their technological choices when enabling eAudiology (Table 1).

Table 1. Guiding Checklist – Assessing and Implementing eAudiology Tools and Technologies

☑ 1. Assess the appropriateness of using eAudiology in your practice.

- Verify whether eAudiology practices have been endorsed by your regulatory college.
- Review guidelines produced by your college about this practice and identify. Restrictions/limitations.
- Review health professional's act requirements for eAudiology practice available in your jurisdiction.
- Identify the application of relevant privacy laws.

☑ 2. Identify the platform(s) that is most suitable for your practice.

- Review the Terms of Use or Service Agreements.
- Identify whether the platform(s) is compliant with privacy legislation in your jurisdiction.
- Understand how and where data is stored, and whether it is subject to secondary use (e.g., marketing analysis).
- Identify how the 3rd party will address privacy/security breaches, including notification of any breach.

☑ 3. Assess the appropriateness of using eAudiology with each patient.

- Confirm the patient is aware of potential limitations to service delivery before use (i.e., tests that cannot be performed remotely, screening vs. diagnostics, etc.).
- Confirm the patient is aware of fees for services/appointments before use.
- Confirm the patient is comfortable with the use of technology (i.e., able to follow instructions, has appropriate dexterity, etc.).

☑ 4. Ensure the patient understands the implications of using eAudiology.

- Obtain and document informed consent from the patient.
- Inform the patient of the risks of potential breaches in privacy/security (e.g., the use of 3rd party platforms). You may wish to share the Terms of Use from the 3rd party with the patient.
- Disclosing to the patient if you have a conflict of interest with the technological platform being used.
- Informing the patient about how information from appointments using eAudiology platforms will be documented.

☑ 5. Implement best practices for the use of technology.

- Develop and enforce good record-keeping practices (i.e., complete reports, document appointment notes, and plan for follow-ups/continuity of care).
- Confirm you have the appropriate technology (i.e., webcam, microphone, Wi-Fi, etc.).
- Ensure that all adjunct staff offering eAudiology care has been trained on the technology.

☑ 6. Reassess your practice/patient needs on an ongoing basis.

Other Practical Tips and Guides

Once a decision has been made to incorporate technology into practice, even if all safeguards are taken to mitigate risk to patients, it is still prudent for clinicians to reflect on how to best ensure that patient privacy is protected. This section is meant to provide additional tips in ensuring the highest level of privacy is offered to patients via connectivity technology. In general, all data that is retained should be collected for a specific purpose. Clinicians should avoid collecting data remotely that is not pertinent to the immediate needs of the remote encounter. While technology offers many benefits, it also offers services that may not be necessary to meet the needs of the patient and that might only serve to create new privacy risks. In other words, when engaging the patient through technology, consideration should be given to what role the technology is filling and to whether the features being offered are beneficial - some features available in fee for service tiers, such as session transcriptions and video conference review, may compromise data security by making information more readily available to a third-party. Although it may be possible to record a session, it may not be prudent or even appropriate if the clinician can take notes for the patient's file throughout the session. Recording sessions is a perk of technology that creates new and, often, unnecessary risks. That said, in some circumstances, the opportunity to record a session may be

advantageous. If so, it is imperative that the patient is properly informed of the risks with this approach and has a right to consent to or decline this service.

Irrespective of the platform used in eAudiology, the best way to safeguard identifiable information is to de-identify patient information whenever possible[15]. For example, if using a computer at a spoke site, avoid entering patient identifying information onto that device. Instead, use a unique identifier that ties a patient back to secure, in-house records that are within the control and oversight of the clinician, not a third-party. If communicating with a patient using a hearing aid manufacturer's module, consider the same strategy. For example, a clinician could use a unique identifier in Noah (or in the manufacturer's software) that links the patient to your clinic's management database. In this way, the platform has information, but it is not linked directly with an identifiable patient.

Consideration must also be given to data storage. This is not simply a matter of ensuring data is stored securely but assessing how long data should be stored. Data that is no longer needed should not be retained. A clinician must consider why data has been recorded and records should not be kept longer than necessary. Data that is out of date or has become irrelevant should not be maintained. A good example of this involves the use of a 'spoke' site computer connected to an audiometer and controlled remotely by a clinician. Once the assessment is complete and the data transferred to the 'hub' site database, the data on the spoke site device should be deleted in such a manner that it can no longer be accessed. Although it may seem obvious, it does bear mentioning that data should never be recorded or stored in an unsecured place. Where possible, data should be encrypted and accessed only through use of a secure password[15]. Patient records should also be reviewed regularly, both by the clinician and the patient. Just like a clinician should vet eAudiology platforms, so too should they review the Terms of Use and compliance with the privacy legislation of cloud storage services.

Conclusion

In summary, audiologists play a key role in protecting the privacy of their patients and ensuring the security of patient health data when using eAudiology. The quagmire of privacy legislation and the borderless nature of videoconferencing and data/information sharing solutions place the clinician in a difficult position. In many cases, audiologists have not been trained to interpret all aspects of privacy legislation that may be applicable in their particular set of practice variables, and may not have the resources to vet every potential platform they work with or are considering. While audiologists must take every reasonable step to mitigate the risk to the patient and themselves when selecting options for remote service delivery, the clinician need not face this challenge alone. They should be able to rely on the developer of the technology they are harnessing to provide a secure product, one that is compliant with the jurisdiction within which it is sold. They should also be able to rely on governments to provide meaningful guidelines to ensure that they meet the expectations of privacy legislation. Finally, audiologists should be able to look to their regulatory colleges for guidance and instruction on privacy legislation and guidelines on the use of technologies of choice. eAudiology is a growing area of virtual health care. Canadian regulatory bodies are lagging in the provision of guidance documents, as the innovation carries on. Future efforts should be devoted to developing resources to educate, train, and support audiologists when using technology-mediated service delivery options such as eAudiology.

References

1. Campos PD, Ferrari DV. Teleaudiology: Evaluation of teleconsultation efficacy for hearing aid fitting. J Soc Bras Fonoaudiol 2012;24(4):301–308. doi:10.1590/S2179-64912012000400003

2. Rushbrooke E, Houston KT. Telepractice in Audiology. San Diego, CA: Plural Publishing; 2016.
3. Montano BJ, Angley G, Ryan-bane C, et al. eAudiology: shifting from theory to practice patient care. A consensus statement on recommendations for telehealth practices in hearing healthcare. Hear Rev 2018;(September):1–8.
4. Olanrewaju RF, Ali NB, Khalifa O, Manaf AA. ICT in telemedicine: Conquering privacy and security issues in health care. eJCSIT 2013;4(1):6.
5. Chaet D, Clearfield R, Sabin JE, Skimming K, on behalf of the Council on Ethical and Judicial Affairs American Medical Association. Ethical practice in telehealth and telemedicine. J Gen Intern Med 2017;32(10):1136–40. doi:10.1007/s11606-017-4082-2
6. Office of the Privacy Commissioner of Canada. The Personal Information Protection and Electronic Documents Act (PIPEDA). https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/. Published September 4, 2019. Accessed May 1, 2020.
7. Office of the Privacy Commissioner of Canada. The Privacy Act. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/. Published September 6, 2019. Accessed May 1, 2020.
8. Office of the Privacy Commissioner of Canada. Summary of privacy laws in Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-2-1. Published May 15, 2014. Accessed April 30, 2020.
9. Ontario. Personal Health Information Protection Act. Ontario.ca. https://www.ontario.ca/laws/view. Published 2004. Accessed May 1, 2020.
10. Government of Canada. Canada Gazette Part I. Canada Gazette. August 3, 2002:1–49.
11. GDPR.EU. General Data Protection Regulation (GDPR) Compliance Guidelines. GDPR.eu. https://gdpr.eu/. Accessed April 30, 2020.
12. Office of the Assistant Secretary for Planning and Evaluation. Health Insurance Portability and Accountability Act of 1996. ASPE. https://aspe.hhs.gov/report/health-insurance-portability-and-accountability-act-1996. Published November 23, 2015. Accessed April 30, 2020.
13. Office for Civil Rights (OCR). The HIPAA Privacy Rule. HHS.gov. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html. Published May 7, 2008. Accessed April 30, 2020.
14. Provincial Health Services Authority. COVID-19 Virtual Health Toolkit. http://www.phsa.ca/health-professionals/professional-resources/office-of-virtual-health/covid-19-virtual-health-toolkit. Accessed April 30, 2020.
15. Information and Privacy Commissioner of Ontario. Thinking about Clouds? Privacy, Security and Compliance Considerations for Ontario Public Sector Institutions. Toronto Ontario; 2016:1-22. https://www.ipc.on.ca/wp-content/uploads/2016/08/Thinking-About-Clouds-1.pdf.