Managing the privacy risks of virtual health care

March 12, 2021

As the COVID-19 pandemic enters its second year, health care institutions are increasingly providing patients and clients with various forms of virtual health care. “Virtual health care” refers to the use of video or audio technology communications to provide non-urgent, non-emergency health care services remotely in real time. Virtual health care services may include medical consults, counselling, coaching, psycho-education, intervention services, and other direct services.

As the Information & Privacy Commissioner of Ontario has observed in its new guideline on the issue, Privacy and security considerations for virtual health care visits (IPC Virtual Care Guideline), the shift to virtual health care has brought with it new privacy and security risks. Many of these risks were difficult to assess adequately in the early stages of the pandemic because health care institutions and providers (together, “institutions”) were working to roll out virtual health care rapidly in the interests of patient welfare. However, now that the initial transition to virtual health care has been made, it may be an opportune time for institutions to revisit these issues.

In this article, we identify some of the privacy and security risks associated with virtual health care and offer general guidance on how they may be managed. In the course of this discussion, we highlight some of the key privacy and security recommendations contained in the IPC Virtual Care Guideline. Although the article focuses largely on virtual health care and health care institutions, many of these recommendations would also apply to social service providers who have made a similar shift towards virtual service provision.

I. What privacy-protecting steps should institutions take when providing virtual health care?

When providing virtual health care services, institutions continue to be subject to the requirements of the *Personal Health Information Protection Act (Ontario)* (PHIPA) in their capacity as health information custodians. As the IPC Virtual Care Guideline observes, these include obligations to contract appropriately with electronic service providers and health information network providers; to collect, use, and disclose Personal Health Information (PHI) only when and to the extent necessary; and to take reasonable steps to safeguard PHI (pp. 2-3).

In the context of virtual health care, the safeguarding requirement means that institutions should consider whether to enact policies governing the use of the virtual health care platform and whether institution staff should be trained on privacy-protecting ways to use the digital platform, such as:

- using only the approved platform to provide virtual health care;
- using only institution-issued or institution-approved devices to provide virtual health care;
- verifying the identity of the patient before starting to provide virtual health care;
- providing virtual health care to patients only from appropriately private locations; and
- not recording the provision of virtual health care services to patients.

The IPC Virtual Care Guideline also recommends additional privacy and security safeguards, including, for example (pp. 6-8):

- installing firewalls and using the latest security and anti-virus software;
- maintaining and monitoring audit logs;
- keeping technology and portable devices containing PHI in a secure location;
- ensuring employees and other agents are appropriately trained in using secure virtual health care platforms and are aware of their ongoing obligation to avoid collecting, using, and disclosing PHI except as necessary;
- adopting a robust system of access controls and ensuring authorizations on a need-to-know basis; and
- providing ongoing security training for employees and other agents and performing regular threat risk assessments.

The IPC Virtual Care Guideline also urges institutions to ensure that their existing privacy and information security policies, breach management protocols, and information security management frameworks address the risks that may arise in connection with providing care through a digital platform (p. 4). Additionally, it provides guidance on the selection of these digital platforms and appropriate contracting with platform providers, and includes a link to the Virtual Visits Solution Standard developed by Ontario Health to facilitate the secure provision of virtual health care (p. 5).

II. What privacy risks should institutions communicate to virtual health care patients through the consent process?

Institutions are encouraged to inform patients ahead of time of some of the potential risks, including privacy-related risks, associated with virtual health care, and to obtain their express consent to receiving virtual health care. For instance, institutions should consider informing their virtual health care patients of the following:

- that the virtual health care services will be made available through third-party platforms, and the ways in which this limits the institution's liability;
- that the use of virtual health care may increase the risk of the patient's identifiable health information being unintentionally disclosed or intercepted by third parties;

- that while the institution will make reasonable efforts to protect the privacy and security of the patient's information, it is not possible to completely secure electronic information and therefore the security and confidentiality of the virtual health care services cannot be guaranteed;
- the safeguards that the institution will follow in order to protect the privacy of the patient information collected and used when providing virtual health care;
- that patients should take steps to protect their privacy when receiving virtual health care (*e.g.* confirming their identity with their health care provider as appropriate; using the virtual health care platform only from a private location, on their own computer or device, and on a password-protected Wi-Fi network; and not recording the virtual health care appointment); and
- that privacy laws will continue to apply, and, accordingly, that patient information may be used or disclosed as permitted or required by law (*e.g.* if there is a risk of harm to an individual or a child is in need of protection under the *Child, Youth and Family Services Act, 2017*).

The IPC Virtual Care Guideline addresses patient consent as well (p. 6).

We recommend that institutions evaluate how best to convey such consent-related information to their virtual health care patients, in light of their business operations and their patient population. They should ensure, at a minimum, that these points are discussed in general terms with each patient during their initial virtual encounter and that the patient is given the opportunity to ask questions before the virtual appointment proceeds. In conjunction with the discussion, it may be appropriate to provide the patient with a written document containing this information and/or directing them to such written information on the institution's website.

III. What precautions should institutions take when emailing with virtual health care patients?

We also suggest that institutions assess the extent to which providing virtual health care will require them to communicate more frequently with patients via email or other electronic means. If it will, consideration should be given to whether such electronic communications can be encrypted. The IPC Virtual Care Guideline is clear on this point, providing, "Custodians should use encryption for emails to and from patients that contain" PHI (p. 9).

Risk assessments, email policies, patient consent

Where encryption is not feasible, the IPC Virtual Care Guideline requires institutions to assess whether using unencrypted email "is reasonable in the circumstances" after considering "all relevant factors," including the sensitivity of the information, the purpose of the transmission, and the urgency of the situation (p. 9). We encourage institutions to capture this assessment in writing and to factor in all relevant considerations, including the types and volumes of PHI contained in the institution's emails to patients and the scope of its email safeguards (discussed further below).

Of note, in 2016 the IPC issued a Fact Sheet entitled Communicating Personal Health Information By Email (IPC Email Fact Sheet), which elaborates on some of the considerations facing health information custodians that wish to use emails with their

patients. The IPC Email Fact Sheet encourages institutions using unencrypted emails to have a written electronic communications policy and to notify patients about the policy (p. 4).

Additionally, the IPC Email Fact Sheet requires institutions to obtain patient consent to the use of unencrypted emails (p. 4). When considering the consent process, we encourage institutions to first determine whether they intend to use unencrypted emails for administrative purposes only (such as appointment scheduling), or also for purposes relating to clinical care (such as communicating with patients about their medications, ongoing symptoms, and the like). On the latter scenario, the types and volumes of PHI being communicated via email, and the commensurate risks associated with using email, will increase. We encourage institutions to approach the consent process with these considerations in mind.

The IPC Email Fact Sheet provides that the consent can take different forms: it can be a self-standing written document, it can be embedded within the form that the patient completes when providing their email address, or it can take the form of a verbal discussion if the individual provides their email address to the institution verbally (p. 4). Another option might be for the consent to be embedded within the online registration for virtual care services. We recommend that institutions adopt a written consent process or ensure that verbal consent is documented in the patient's record.

Regardless of the purposes for which unencrypted emails are to be used, we suggest that institutions consider addressing the following in their consent discussions and documentation:

- that, with the patient's consent, the institution may send the patient text messages, email or other forms of electronic communication, and the purposes for which the institution may send such messages (*i.e.* appointment scheduling and confirmation, patient care, *etc*.);
- the patient's consent options, so that the patient can choose the circumstances in which they consent to receiving unencrypted emails (*e.g.* they may agree to receive administrative emails only, or emails pertaining to their clinical care as well) (see the IPC Email Fact Sheet p. 4);
- that response times to electronic communications from patients cannot be guaranteed, and that therefore patients should not communicate electronically in emergency situations or where an urgent response is required;
- that electronic communications may be forwarded to those involved in the delivery and administration of care (*e.g.* staff who are scheduling appointments) but will not be forwarded to third parties, including family members, without the patient's consent or except as authorized or required by law; and
- that the privacy risks associated with virtual health care also apply to the use of electronic communications, and that there are additional risks associated with use of electronic communications (*e.g.* an increased risk of being misdirected, received by unintended recipients, forwarded or circulated without the patient's or institution's knowledge, or accessed on portable devices (*e.g.* cell phones, laptops) that are more vulnerable to theft and loss).

Email safeguards

Finally, if the shift to virtual health care is likely to bring about an increase in unencrypted email communications with patients, we recommend that institutions consider the state of their email safeguards. For instance, it may be appropriate to train institution staff on the importance of avoiding or minimizing PHI when emailing with patients and on double checking email addresses prior to sending emails out. The IPC Virtual Care Guideline lists additional safeguards to consider in connection with electronic communications that may contain PHI, such as (pp. 8-9):

- notifying patients in the email that the information received is confidential, and providing them with instructions to follow if an email is received by mistake;
- confirming that email addresses are up to date;
- restricting access to the email system and to email content on a need-to-know basis; and
- storing PHI on servers only for as long as is necessary for the intended purpose.

IV. Conclusion

Institutions have done a great deal to roll out virtual health care during a stressful and rapidly evolving time in health care. They are to be commended. Now that the widespread rollout has taken place, and the shift to virtual health care shows no sign of slowing down, it may be wise to pause, consider some of its potential privacy and security risks, and assess how best to manage and mitigate those risks going forward. This article intends to help with that important process.

By

Ira Parghi, Tanvi Medhekar

Expertise

Disputes, Health Care, Health Care Disputes, Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749