

**• BALANCING PRIVACY AND CONVENIENCE: MEDICAL INFORMATION AND THE EMERGENCE OF VIRTUAL MEDICINE<sup>1</sup> •**

Valerie Prather, Partner, Barbara Stratton, Partner, Marin Leci, Associate, Kees de Ridder, Associate, and Melanie Mireault, Associate, Bennett Jones LLP  
© Bennett Jones, Calgary and Edmonton



**Valerie Prather**



**Barbara Stratton**



**Marin Leci**



**Kees de Ridder**



**Melanie Mireault**

**Online** healthcare service provider, Babylon Health developed an app that connects physicians and other healthcare professionals with patients through remote video or audio consultations. Babylon Health is one of many players in the growing global market of virtual healthcare, driven by the desire for change in the delivery of healthcare.

In light of the COVID-19 pandemic, demand for virtual healthcare platforms such as apps has exponentially increased. However, the increasing use of virtual healthcare platforms is not without risks. On June 9, 2020, Babylon Health advised that its app had suffered a data breach. One of Babylon Health’s UK-based users discovered he had access to a video recording of a consultation between a physician and a patient. The Babylon breach resulted from a software error rather than a malicious attack and Babylon

Health was able to resolve the issue quickly. Babylon Health stated that a limited number of users in the United Kingdom were affected by the software issue, leading to one user viewing the initial part of a video consultation of another user.

The increasing use of virtual healthcare platforms raises questions and concerns about the protection of personal health information and the application of privacy legislation. Specifically, what happens if a virtual healthcare platform or app experiences a data breach in Alberta? Who bears the responsibility for such a risk?

**VIRTUAL HEALTHCARE IN ALBERTA**

Residents in Alberta can access healthcare virtually, either through telehealth services provided by Alberta

Health Services<sup>2</sup>, or through privately developed apps like the Babylon app. Virtual platforms allow healthcare professionals to interact with patients in real time without requiring physical interaction, which has obvious appeal in during a pandemic.

Below we focus on apps that are conceptually similar to the Babylon app to consider how privacy laws will apply to Alberta residents and doctors who utilize virtual healthcare technology. However, the legislation and risks discussed below will likely apply to other virtual platforms that connect patients and physicians.

## ALBERTA'S PRIVACY LEGISLATION

### *HEALTH INFORMATION ACT*

The *Health Information Act (HIA)*, RSA 2000, c H-5, sets out the rules that apply for the collection, use, disclosure, and protection of health information in Alberta.

Under the *HIA*, the “custodian” of health information has a duty to protect that information. For healthcare apps similar to the Babylon app, the licensed doctor providing healthcare services would generally be the custodian of the “health information” shared on the app (As regulated members of the College of Physicians and Surgeons of Alberta, doctors are custodians of health information under the *HIA*; see *Health Information Regulation*, Alta Reg 70/2001, s 2(2)(i)). Health information captures medical records accessed through the app, including any consultation notes, prescriptions or referrals. Physician video or audio consultations that are recorded and accessible through the app would also constitute health information under the *HIA*.

Much like physicians who provide in-person services, physicians providing virtual health services have a duty to take reasonable steps to maintain proper safeguards to protect patients’ information shared through apps or other virtual platforms (*HIA*, s 60). As information managers that process and store health information, the app provider would be an “affiliate” of the custodian (ss 1(1)(a)(iv) and 66(1)). While the affiliate must comply with the *HIA* and

ensure health information is protected, the custodian ultimately remains responsible for compliance with the *HIA* (s 66(6)). As a result, any privacy breach could generate liability for both the custodian and the affiliate. Accordingly, while app users give their health information to an affiliate (for example, by filling out forms or providing medical history through the app), for the purposes of the *HIA*, an app user will be considered to have provided the information directly to the physician. A physician must take reasonable steps to ensure such information is secure.

Should a data breach occur on a virtual healthcare platform resulting in unauthorized disclosure of individually identifying health information, the affiliate (i.e., the app provider) must notify the custodian (i.e., the doctor(s), or other custodian(s) such as Alberta Health Services, as applicable) as soon as practicable. Subject to some exceptions, the custodian must then notify the:

- Information and Privacy Commissioner of Alberta;
- Minister of Health of Alberta; and
- The individual who is the subject of the individually identifying health information. (*HIA*, s 60.1. An exception exists whereby a custodian does not need to give notice to the individual who is the subject of individually identifying health information where the custodian considers that such notice could reasonably be expected to result in a risk of harm to the individual’s mental or physical health.)

In sum, if a data breach occurs (whether through a malicious action, mistake, software issue, or otherwise) and health information is disclosed, the physician providing services through a virtual platform bears the responsibility for the breach.

The *HIA* does not require a standard of perfection; physicians have a duty to take reasonable steps to make sure proper safeguards are in place. Despite taking reasonable steps to safeguard information, breaches may still occur.

If a breach occurs, the Commissioner will consider whether the custodian and, by extension the affiliate,

took reasonable steps, and will look at (among other things) the privacy impact assessment provided by the custodian (as required by s 64(1)), policies in place, and information management agreements with the affiliate (as required by s 66). Courts have the ability to enforce the Commissioner's orders. A custodian may be found guilty of an offence or fined in accordance with the *HIA* (s 107), should a Court determine that a custodian:

- Failed to take reasonable steps safeguard medical information and data;
- Failed to comply with an order made by the Commissioner; or
- Failed to disclose the unauthorized use of health information.

#### *PERSONAL INFORMATION PROTECTION ACT*

Alberta's private sector privacy laws, the *Personal Information Protection Act (PIPA)*, SA 2003, c P-6.5., may also apply to data breaches that occur through virtual healthcare platforms, such as apps, regardless of whether the breach relates to health information. In this case, the app or virtual service provider would likely be responsible for any breaches resulting in the release of personal information.

#### INFORMATION TRANSFERRED OUTSIDE ALBERTA

If the virtual healthcare platform transfers or ultimately stores personal information or health information outside Alberta, the protection of that information may also be subject to the laws of the jurisdiction where that data is ultimately transferred or stored. In addition, federal privacy laws, such as the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, may apply. If information is transferred outside of Canada, other legislation may apply based on where the information is ultimately transferred.

#### INSIGHTS

Virtual healthcare services, like video consultation apps, present an opportunity to reduce or eliminate

barriers to accessing primary care resources. However, as the use of virtual medicine continues to expand, the risks highlighted above will continue to play a key role in driving the level of physician buy-in and public reliance on virtual healthcare platforms.

The Babylon breach underscores the reality that, ultimately, data breaches may occur regardless of the steps taken by virtual healthcare platforms to secure sensitive information and data. An awareness of the risks, coupled with the development a plan of action that is in place *before* a data breach occurs can serve to mitigate the legal risks associated with data breaches.

Before entering this space, physicians and companies developing virtual healthcare platforms should carefully consider the applicability of privacy legislation and prioritize the development of mitigation strategies designed to reduce or eliminate the risk associated with the use and transfer of sensitive information over virtual platforms.

*[Valerie Prather is a Partner with Bennett Jones' Calgary office. Her practice focuses on professional negligence and administrative law. She has appeared before various administrative tribunals, the Court of Queen's Bench and the Court of Appeal of Alberta. Ms. Prather can be reached at pratherv@bennettjones.com.]*

*Barbara Stratton is a Partner with Bennett Jones' Edmonton office. She supports clients navigating the complex aspects of wills and estate litigation, assists employers and employees on all aspects of employment law from inception to termination, and represents physicians and surgeons on medical malpractice cases and a variety of other health law issues. Ms. Stratton can be reached at strattonb@bennettjones.com.]*

*Marin Leci is an Associate with Bennett Jones' Calgary office. Mr. Leci maintains a general commercial litigation practice with an emphasis on corporate commercial disputes, energy industry disputes, and professional liability matters. He can be reached at lecim@bennettjones.com.]*

*Kees de Ridder is an Associate with Bennett Jones' Calgary office. He has a general commercial practice with a focus on intellectual property. His experience*

*includes advising physicians on privacy matters and cybersecurity, and supporting inventors in the medical industry with the commercialization and patenting of their technology. Kees can be reached at [deridderk@bennettjones.com](mailto:deridderk@bennettjones.com).*

*Melanie Mireault is an Associate with Bennett Jones' Calgary office. She has a general corporate*

*commercial law practice with a focus on commercial transactions. Ms. Mireault can be reached at [mireaultm@bennettjones.com](mailto:mireaultm@bennettjones.com).]*

---

<sup>1</sup> This article was first published as a blog on Bennett Jones' website on June 24, 2020.

<sup>2</sup> <https://www.albertahealthservices.ca/info/page15734>.