Office of the Information and
Privacy Commissioner of Alberta

Investigation Report H2021-IR-01

Investigation into the use of Babylon by TELUS Health by Alberta physicians

July 29, 2021

Babylon Health Canada Ltd. (Dr. Keir Peterson, Alberta Lead Physician), Dr. Ryan Wei, Dr. Denise Michelle Eckenswiller, Dr. Wenshuang Nie, Dr. Matthys Cornelius Van Schalkwyk, Dr. Michael Yosefi, Dr. Helen Qian, Dr. Haitham Kharrat, Dr. Keshav Sharma, Dr. Islam Elawadly, Dr. Roopinder Kaur Dulai, Dr. Jacqueline Jenkins, Dr. Joseph Kumpula, Dr. Sanjeeve Sockanathan and Dr. Harley Thomas Syyong

Investigations 015679, 016738, 016739, 016740, 016741, 016742, 016743, 016744, 016745, 016746, 016747, 016748, 016749, 016750 and 016751

Commissioner's Message

In March 2020, the Government of Alberta (GoA) issued a news release for the Babylon by TELUS Health app describing it as "a new tool for Albertans to access health-care information and support in response to COVID-19 – from anywhere in the province." The news release said, "The service is being delivered to Albertans through an alternative relationship plan (ARP) between the Alberta government and TELUS."

The GoA's announcement resulted in a number of media articles, as well as questions from the media and public directed to my office, concerning the app. Shortly after the announcement, I received a letter from the NDP Official Opposition requesting that I "evaluate" the app for compliance with Alberta's privacy laws. I also received requests from members of the public to investigate the app.

Given the above, and considering the app was already in use in Alberta, I initiated investigations of Babylon Health Canada Limited (Babylon) under Alberta's *Health Information Act* (HIA) and the *Personal Information Protection Act* (PIPA). I later extended the HIA investigation to include the 14 physicians that were employed by or contracted to Babylon at the time the initial investigation was launched. I did this because Alberta's HIA applies to health custodians (physicians), and sets out specific duties and obligations that custodians must comply with.

The HIA investigation examined six compliance issues and found the custodians did not meet the requirements of the legislation for any of them. Some key findings:

- Although Babylon had an extensive suite of general policies and procedures in place, the custodians did not meet their legal obligation to establish or adopt policies and procedures to facilitate the implementation of HIA and the Regulations.
- The custodians did not prepare and submit (or endorse) a privacy impact assessment prior to adopting the Babylon application to provide health services.
- The custodians did not enter into an information manager agreement with Babylon Health Canada, and did not meet the requirements of the *Health Information Regulation* with respect to health information that is stored or used in jurisdictions outside Alberta. In particular, the custodians did not enter into agreements that would ensure they retained control over health information they collected, used or disclosed as part of providing health services through the Babylon app.
- The custodians did not comply with HIA's requirements to limit the collection and use of health information to what is essential to enable the custodians' purposes. In particular:
    - Collecting and using copies of government-issued identification and selfie photos from patients through the Babylon app goes beyond what is essential to verify identity and provide health services. Other simpler, effective methods exist for this purpose, and are consistent with provincial and federal guidelines for verifying identity for virtual health care purposes.
    - Collecting (recording) and using audio and video consultations through the Babylon app goes beyond what is essential to provide a health service and, again, is not consistent

with provincial and federal guidelines for providing virtual health care.
  - Collecting location information is not essential to provide a health service.

During the investigation, we were advised that, "[O]n January 18th, 2021, TELUS acquired the Canadian operations of Babylon Health. The acquisition includes all of the Canadian operations, including the clinic, and we have licensed from Babylon the software platform upon which the virtual service runs. From a privacy perspective, this means that the Babylon operations in Alberta are now part of TELUS and will now be operating under the TELUS privacy program." We were also informed of steps that have been taken to address a number of the compliance issues identified through the investigation, including:

- Babylon policies have been replaced with new TELUS Health MyCare policies, which outline the responsibilities of the physicians and their affiliates under HIA. An Alberta-specific Custodian Privacy & Security Policy Manual (to which all relevant policies are appended) has been developed.
- An updated PIA is being prepared that addresses the requirements outlined in my office's Privacy Impact Assessment Requirements document. Babylon physicians will be required to review and endorse the PIA.
- Babylon has entered into an information manager agreement (IMA) with the custodians.
- Physicians completed updated training that includes references to HIA and its associated requirements. TELUS Health MyCare privacy and security awareness training has been developed to also meet this requirement.

I appreciate the steps that have been taken to date, and have requested that the physicians report back within six months on progress complying with the remaining outstanding recommendations.

This investigation is an important reminder that Alberta's HIA makes **custodians** responsible for health information they collect, use and disclose when providing health services, whether virtually or in person. In this case, the physician custodians offered health services through a technology solution without ensuring they were doing so in compliance with Alberta's law. Ultimately, HIA makes the physician custodians responsible and accountable for the health information of their patients, including when they engage technology service providers both within and outside of Canada.

We are seeing widespread and accelerated development and implementation of virtual healthcare technologies as a result of the pandemic. Custodians who are involved in these initiatives must be mindful of their legal obligations with respect to the collection, use, disclosure and protection of health information. The rules established by Alberta's HIA are important for engendering public trust and confidence in the health care system, and these rules are especially important when new technologies, such as virtual care solutions, are implemented.

Jill Clayton
Information and Privacy Commissioner

Table of Contents

Introduction

[1] On May 22, 2019, the Office of the Information and Privacy Commissioner (OIPC) received a privacy impact assessment (PIA) from Dr. Keir Peterson, Medical Director and subsequently Alberta Lead Physician of Babylon Health Canada Limited (Babylon). The PIA was for the Babylon by TELUS Health – Business to Business (B2B) product. The OIPC opened case file #012533.

[2] On June 18, 2019, the OIPC received another PIA from Dr. Keir Peterson regarding Babylon's "implementation of Netcare". The OIPC opened case file #013187.

[3] On March 6, 2020, the OIPC received a PIA from Dr. Renie Traiforos, who was identified in the PIA as the Alberta Physician Lead for Babylon. The PIA was for the Babylon by TELUS Health – Business to Consumer (B2C) product. The OIPC opened case file #015535.

[4] On March 16, 2020, the OIPC wrote to Babylon advising that it had completed its review of Babylon's Netcare implementation PIA (case file #013187), but the PIA was not accepted as it did "not provide sufficient details".

[5] On March 19, 2020, the Government of Alberta (GoA) issued a news release for the Babylon by TELUS Health app, describing it as follows:[1]

> Babylon by TELUS Health is a service already available in British Columbia via a free downloadable app. The app can serve as a new tool for Albertans to access health-care information and support in response to COVID-19 – from anywhere in the province. Albertans can use the service to check symptoms, book appointments, see a doctor, and get prescriptions and referrals for diagnostic imaging and specialists – all covered by Alberta Health Care.
>
> …
>
> The service is being delivered to Albertans through an alternative relationship plan (ARP) between the Alberta government and TELUS. There are currently 61 ARPs in Alberta involving 2,500 doctors.

[6] Throughout March 2020, a number of articles concerning the Babylon by TELUS Health app were published by various media outlets.[2,3]

[7] Subsequently, the OIPC received questions from media and the public asking whether TELUS, Alberta Health or GoA completed PIAs for the app. Members of the public wrote to the Commissioner on March 22, 2020 and March 25, 2020 requesting "an urgent and immediate investigation" of this "novel and potential non-compliant collection, use and disclosure of [Albertans] personal and health information", and saying, "Please review

[1] Government of Alberta, "New app helps Albertans access health care", March 19, 2020.
[2] Alberta Medical Association, "Babylon: setting the record straight", March 21, 2020.
[3] Hardcastle, L. and Ogbogu, U, "Opinion: Alberta's virtual health-care app plagued with problems", Edmonton Journal, March 26, 2020.

and launch an investigation on Babylon, a new 'app-based healthcare service' offered by Telus".

[8] On March 23, 2020, the Commissioner received a letter from MLA David Shepherd, Health Critic, NDP Official Opposition, which said, in part:

> Babylon's terms and conditions and privacy policy are cause for concern. Our caucus has heard from Albertans and we are seeking a formal evaluation from your Office regarding whether or not the Terms and Conditions, and the Privacy Policy, are compliant with legislation in Alberta.

[9] On April 20, 2020, the OIPC wrote to Babylon advising it would not accept PIAs #012533 and #015535. Each letter stated:

> The PIA does not describe the relationship between custodians and Babylon. In addition, the privacy risk assessment fails to provide adequate detail and the required policies and procedures are incomplete. The information submitted also describes the over collection of personal information including the collection of copies of [drivers'] licenses.

[10] Given all of the above, and considering the app was in use in Alberta, the Commissioner wrote to Babylon on April 20, 2020 advising she was opening investigations of the Babylon by TELUS Health virtual healthcare app (the app) under section 36(1)(a) of the *Personal Information Protection Act* (PIPA) and section 84(1)(a) of the *Health Information Act* (HIA). These sections of PIPA and HIA allow the Commissioner to conduct investigations to ensure compliance with any provision of the Acts.

[11] The Commissioner's letter with respect to the HIA investigation said:

> Several factors led me to opening this investigation under HIA. In addition to concerns identified during my office's review of the privacy impact assessment you had submitted on the app … there has been considerable public attention regarding the app's compliance with privacy laws and I have received requests for investigation.

[12] On August 17, 2020, the Commissioner also opened investigations of the 14 physicians that were employed by or contracted to Babylon at the time the initial investigation was launched on April 20, 2020.

[13] I was assigned to conduct the investigations.

[14] In January 2021, I was advised that, "[O]n January 18th, 2021, TELUS acquired the Canadian operations of Babylon Health. The acquisition includes all of the Canadian operations, including the clinic, and we have licensed from Babylon the software platform upon which the virtual service runs. From a privacy perspective, this means that the Babylon operations in Alberta are now part of TELUS and will now be operating under the TELUS privacy program."

[15] Despite this, my investigations are concerned with the operation and implementation of the app and its use by the 14 physicians at the time this investigation was initiated. This report sets out the findings and recommendations from my investigations.

Background

[16] The Babylon by TELUS Health app is described in Babylon's Terms and Conditions document, which says that Babylon's "Services" include "digital healthcare tools" as well as "Clinical Services".

[17] The digital healthcare tools (which, at the start of this investigation, included "Symptom Checker" and "Healthcheck")...

> ...provide healthcare information and **not medical advice, diagnosis and/or treatment**. If you choose to submit details about your symptoms in the App, the information returned to you is general health information and no Practitioner is involved in providing the information. Our information services are not a substitute for a doctor or other healthcare professional. [emphasis added][4]

[18] These digital healthcare tools were not reviewed as part of this investigation, but are the subject of OIPC Investigation Report P2021-IR-02 under PIPA.

[19] The Terms and Conditions document defines "Clinical Services" as "video and audio consultations with our Practitioners". Clinical services are available in some provinces, including Alberta, and include:

- remote video and voice consultations with our Practitioners;
- where appropriate through use of our Clinical Services, our Medical Professionals may prescribe medicines (see section H);
- access to healthcare records we hold; and
- access to other digital healthcare tools that provide health and lifestyle information.

[20] "Practitioners" include "Medical Professionals" and "Allied Professionals", described as follows:

- Medical Professionals are family physicians licensed with the physician regulatory body in their province and/or territory of practice, who have committed to provide Services in accordance with clinical best practice and applicable professional standards.

- Allied Professionals are registered with the applicable regulatory body in their province and/or territory of practice and have committed to provide Services in accordance with best practice and applicable professional standards.

[21] In Alberta, the app allows users to book appointments with Practitioners that are "Family Doctors", "Mental Health Counsellors" and "Registered Dietitians".

[22] All of the above services are provided through two product offerings: Business to Consumer (B2C) and BusinessPLUS by Babylon by TELUS Health (B2B). The B2C product is the primary consumer offering, obtained by a free download. The B2B product is provided by employers to employees at either a discounted rate or at no cost to the employee; users may access its features by entering a code provided by their employer.

[4] Where this report directly cites submissions made by Babylon, Babylon UK or the physicians, any emphasis has been added, except where otherwise stated.

Jurisdiction

Babylon Partners Limited (UK) and Babylon Health Canada Ltd.

[23] Babylon Partners Limited (UK) (Babylon UK) is headquartered in London, United Kingdom, and is "a global organisation in digital health that combines the benefits of [Artificial Intelligence] with the medical expertise of doctors"[5]. Babylon UK describes its product/services as follows:

> …Babylon [UK] uses a combination of AI technology and medical expertise to deliver 24-hours-a-day, 7-days-a-week access to digital health tools (including health assessment, triage and medical information tools), to people across Europe, North America, Asia, the Middle East and Africa, as well as video doctor consultations.

[24] Babylon UK established Babylon Health Canada Ltd. (Babylon) to provide the Babylon by TELUS Health app to Canadians.

[25] Babylon is registered as an extra-provincial corporation in British Columbia. It has physical administrative offices in Vancouver and Toronto and provides services in a number of Canadian jurisdictions, including Alberta.

Custodians (Physicians)

[26] HIA applies to "custodians" in respect of the collection, use and disclosure of "health information".

[27] Section 1(1)(f)(ix) of HIA defines "custodian" to include a "health services provider who is designated in the regulations as a custodian". Section 2(2)(i) of the *Health Information Regulation* (HIA Regulation) designates regulated members of the College of Physicians and Surgeons of Alberta as custodians.

[28] At the start of this investigation, there were 14 Alberta-based physicians associated with Babylon. Twelve of the physicians were employed by Babylon in the position of "Family Physician (Digital Healthcare)", with start dates ranging from July 2019 to April 2020. Two others had entered into Family Physician Self Employed Consultancy Agreements, with start dates ranging from March to April 2020.

[29] All of the physicians are regulated members of the College of Physicians and Surgeons of Alberta; this is, in fact, a requirement of their employment or consultancy with Babylon according to the associated agreements.

[5] From Babylon UK submission for this investigation, received May 14, 2020.

[30] The physicians are, therefore, custodians as defined in section 1(1)(f)(ix) of HIA.[6]

Health Information

[31] "Health information" is defined in section 1(1)(k) of HIA and includes "diagnostic, treatment and care information" as well as "registration information".

[32] "Diagnostic, treatment and care information" is further defined in section 1(1)(i) of HIA as follows:

> (i) "diagnostic, treatment and care information" means information about any of the following:
>
> (i) the physical and mental health of an individual;
> (**ii) a health service provided to an individual** [emphasis added]

[33] "Registration information" is defined in section 1(1)(u) of HIA as follows:

> (u) "registration information" means information relating to an individual that falls within the following general categories and is more specifically described in the regulations:
>
> (i) demographic information, including the individual's personal health number;
> (ii) location information;
> (iii) telecommunications information;
> (iv) residency information;
> (v) health service eligibility information;
> (vi) billing information

[34] As noted above, 12 of the physicians associated with Babylon are employed in the position of "Family Physician (Digital Healthcare)". The employment agreement does not specifically describe the duties of this position, but it is clear these physicians are engaged in providing health services to individuals, including diagnosis, treatment and care as defined in HIA. Any information produced in the course of providing these health services is health information as defined in section 1(1)(k) of HIA.

[35] Two of the physicians associated with Babylon have entered into Family Physician Self Employed Consultancy Agreements. These agreements are between Babylon and the physicians' corporations. "Schedule 1 - Services" of the consultancy agreement says:

> The Services to be undertaken by the Consultant in relation to this agreement shall include:
>
> - <u>To be engaged as a medical practitioner in order to carry client/patient consultations at home as required</u>…

[6] Babylon also offers Clinical Services consultations with dietitians and mental health counsellors; however, these services are not subject to HIA as these professionals are not custodians as defined in the Act. They are, however, the subject of OIPC Investigation Report P2021-IR-02 under PIPA.

- To carry out the above client/patient consultations in accordance with the specifications as set out in the Client's [Babylon's] Clinical Handbook, the Policies and Procedures manual (as updated from time to time) and in accordance with generally accepted standards of good practice,

- To produce medical reports as part of the consultations within the specified time limits.

[36] It is clear these consultant physicians are engaged in providing health services to individuals, including diagnosis, treatment and care. Information collected, used and disclosed by these physicians in the course of providing health services is health information as defined in section 1(1)(k) of HIA.

Affiliates

[37] Section (1)(1)(a)(iii) of HIA defines an "affiliate" as, among other things, "a person who performs a service for the custodian as an appointee, volunteer or student **or under a contract or agency relationship with the custodian**" [emphasis added].

Babylon Health Canada (Babylon)

[38] The custodian physicians in this investigation described their relationship with Babylon as follows:

> Babylon provides the Babylon by TELUS Health app. As an employee of Babylon, Physicians provide health care (clinical) services to Alberta residents through the app. To support provision of clinical services, Babylon provides physicians with access to its technology platform and related IT, information management and administrative and clinical support services including video consultation technology, appointment booking software, prescription fulfillment technology and any associated technological updates, maintenance, quality control and support. Babylon hires clinical and administrative support to assist in the provision of services.

[39] Babylon has entered into employment or consultancy agreements with the physicians, who are custodians as defined in HIA. Babylon in effect operates and manages the virtual clinic and employs staff to provide services to support physicians practicing at the virtual clinic.

[40] Given the above, Babylon is an affiliate of the physicians who are employed or contracted by Babylon as Family Physicians (Digital Healthcare), as contemplated by section (1)(1)(a)(iii) of HIA.

[41] Pursuant to section 62 of HIA, the physicians are responsible to ensure their affiliates comply with HIA and its regulations, as well as any policies and procedures. Further, "Any collection, use or disclosure of health information by an affiliate of a custodian is considered to be collection, use or disclosure by the custodian" (section 62(3)).

[42] Babylon is also an "organization" as defined under section 1(1)(i) of PIPA, such that PIPA would apply to Babylon's collection, use and disclosure of **personal information** in Alberta.

[43] However, section 4(3)(f) of PIPA states that PIPA "does not apply to the following: (f) health information as defined in the *Health Information Act* to which that Act applies." As the information at issue in this matter is health information as defined in HIA to which HIA applies, PIPA does **not** apply to this information.

TELUS Health Solutions Inc. (TELUS)

[44] As previously noted, an "affiliate" includes "a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian". An affiliate can also be "**an information manager** as defined in section 66(1)" of HIA (section 1(1)(a)(iv)) [emphasis added].

[45] Section 66(1) of HIA says an information manager means:

> 66(1) …a person or body that
>
> (a) processes, stores, retrieves or disposes of health information,
> (b) in accordance with the regulations, strips, encodes or otherwise transforms individually identifying health information to create non-identifying health information, or
> **(c) provides information management or information technology services.** [emphasis added]

[46] The physician custodians in this case advised me:

> Babylon provides the Babylon by TELUS Health app. As an employee of Babylon, Physicians provide health care (clinical) services to Alberta residents through the app. To support provision of clinical services, Babylon provides physicians with access to its technology platform and related IT, information management and administrative and clinical support services including video consultation technology, appointment booking software, prescription fulfillment technology and any associated technological updates, maintenance, quality control and support.

[47] These are "information management" and "information technology" services. In providing these services to the custodian physicians, Babylon is an information manager as defined in section 66(1) of HIA.

[48] In order to provide these services, Babylon has a contractual agreement with TELUS Health. Article 5 of the "Contractual Agreement between Babylon and TELUS" describes the relationship as follows:

> 5.1 Managed Services
>
> (a) TELUS will provide babylon, as subcontractor to TELUS, access to the TELUS Health Cloud Platform account… for the sole purposes of hosting, operating, and making available all services provided to and through the babylon App including the AI Information Services to Individual End Users via the Babylon [sic] App and the Health Professional Portal and the AI Information Services made available via the Health Professional Portal, to Health Professional Customers…
> (b) The Managed Services are described at a high level in Schedule D.

[49] Article 5 of the Contractual Agreement, and excerpts from Schedule D to the Agreement (which were provided for my review), confirm that TELUS provides information management and information technology services to Babylon; Babylon, in turn, provides these services to the custodian physicians, as an affiliate and information manager.

[50] As stated in OIPC Investigation Report H2014-IR-01, "HIA does not provide specific guidance to custodians regarding subcontracting arrangements their information managers may make, but the HIA does impose a duty on information managers to comply with the HIA and with the terms of their agreement with the custodian (section 66(5) of the HIA)".[7] Therefore, as an information manager to the 14 custodians, it is the responsibility of Babylon to ensure it takes reasonable steps to ensure appropriate safeguards are in place to protect the privacy of health information that is transmitted to or stored by its subcontractors.

Babylon UK and Third Party Service Providers

[51] As noted above, Babylon UK is the parent company to Babylon, and established the latter to provide the Babylon by TELUS Health app to Canadians.

[52] With respect to its relationship with Babylon, Babylon UK explained:

> The Babylon Canada platform may share data with Babylon Partners Limited (a group company based in London, United Kingdom, where Babylon is subject to and complies with the GDPR/UK Data Protection Act 2018) for the purposes of delivering services and providing technical support and maintenance.
>
> ...Selected staff at Babylon Partners Limited may access data in order to troubleshoot technical issues for the service.

[53] Given that Babylon "shares data" with Babylon UK "for the purposes of [the latter] delivering services and providing technical support and maintenance" and "in order to troubleshoot technical issues for the service", it appears that Babylon UK provides information management and information technology services to Babylon; Babylon, in turn provides these services to the custodian physicians, as an affiliate and information manager.

[54] Babylon UK also engages a number of service providers to provide support and functionality associated with the app. These service providers work together with Babylon UK to provide the application to individuals, including individuals in Canada. I asked Babylon to provide information regarding these third party service providers, and received the following response on May 25, 2020 from Babylon UK:

> Babylon uses a range of third-party software and services to deliver its platform, and this is how all software is built. Where the platform integrates with third party services, the service provider often

[7] Office of the Information and Privacy Commissioner of Alberta, "H2014-IR-001: Medicentres Canada Inc.", August 26, 2014.

> provides software to integrate with their service, that may or may not be open source. Most of the third-party software that Babylon uses is open-source software, which does not collect any personal information. Use of this software is subject to internal policies.

[55] Babylon provided a listing of over 20 third-party service providers. The purposes for which these providers are engaged, include:

- Address validation
- Application analytics
- User authentication
- Infrastructure
- Technical support, service management
- Document storage
- Payments
- Application error reporting
- Call centre communications
- Centralised logging
- Translations
- Personal health number validation and billing
- Email
- Technical analytics & performance
- Identification validation
- On-call support
- eFaxes
- Application messaging
- Testing
- Marketing
- Voice conferencing and SMS
- Video conferencing
- Clinical support

[56] These third parties have agreements with Babylon UK to provide software and services necessary to deliver the app; Babylon UK, in turn, provides these services to Babylon; Babylon provides these services to the custodian physicians, as an affiliate and information manager.[8]

[57] Again, as noted above, HIA does not provide specific guidance to custodians regarding subcontracting arrangements their information managers may make, but section 66(5) of HIA does impose a duty on information managers to comply with HIA and with the terms of their agreement with the custodian (section 66(5) of HIA). Therefore, as an information manager to the 14 custodians, it is the responsibility of Babylon to take

[8] These agreements are reviewed in more detail later in this report. See Issue 4.

reasonable steps to ensure appropriate safeguards are in place to protect the privacy of health information that is transmitted to or stored by its subcontractors.

[58] Further, section 66(6) of HIA says that "a custodian continues to be responsible for compliance with this Act and the regulations in respect of the information provided by the custodian to the information manager". That is, the physician custodians are ultimately responsible to ensure their information manager (Babylon) complies with HIA, including with respect to subcontracting relationships Babylon may have with Babylon UK and other third party service providers.

Issues

[59] The following issues were identified for this investigation:

- Issue 1: With respect to services provided under employment or contract with Babylon, have the custodians (physicians) established or adopted policies and procedures as required by section 63 of HIA?

- Issue 2: With respect to services provided under employment or contract with Babylon, have the custodians (physicians) prepared privacy impact assessments as required by section 64 of HIA?

- Issue 3: With respect to services provided under employment/contract with Babylon, have the custodians (physicians) entered into agreement(s) with an information manager, as required by section 66 of HIA and 7.2 of the *Health Information Regulation*?

- Issue 4: Have the custodians (physicians) met the requirements of section 8(4) of the *Health Information Regulation* with respect to health information that is stored or used by a person in a jurisdiction outside Alberta?

- Issue 5: Have the custodians (physicians) taken reasonable steps to maintain administrative and technical safeguards to protect health information as required by sections 60 and 63 of HIA, and section 8 of the *Health Information Regulation*?

- Issue 6: Do the custodians (physicians) collect, use and disclose health information in a limited manner as required by section 58 of HIA?

Methodology

[60] I took the following steps during the course of this investigation:

- Held meetings and communicated in writing with Babylon, Babylon UK and TELUS representatives, as well as communicated in writing with the physicians[9]
- Sent written questions to and reviewed responses from Babylon and the physicians
- Requested and reviewed copies of documentation, including policies, procedures, data flows, contracts and risk assessments
- Reviewed the two PIAs submitted by Dr. Keir Peterson, and the PIA submitted by Dr. Renie Traiforos
- Sent a draft investigation report to Babylon and the physicians for fact checking, considered feedback and finalized the report

[9] When the investigation began, Babylon UK provided information on behalf of Babylon. During the course of the investigation, Babylon provided information related to the investigation directly. The physicians authorized Babylon to respond on their behalf.

Analysis, Findings and Recommendations

Issue 1: With respect to services provided under employment or contract with Babylon, have the custodians (physicians) established or adopted policies and procedures as required by section 63 of HIA?

[61] Section 63 of HIA says:

> 63(1) Each custodian must establish or adopt policies and procedures that will facilitate the implementation of this Act and the regulations.

[62] I asked the physicians whether, in respect of their work with Babylon, they had established or adopted policies and procedures to facilitate implementation of HIA and the regulations, as required by section 63 of HIA. In response, the physicians provided me with a document entitled "Babylon Policies – Canada". The document contains the following policies*:*

- "Privacy Accountability Policy"
- "Training Policy"
- "Research Policy"
- "Monitoring and Audit Policy"
- "Data Access Request Policy"
- "Third Party Policy"
- "Records, Retention and Disposal Policy"
- "Information Classification and Handling Policy"
- "Risk Assessment and Treatment Policy"
- "Network and Security Policy"
- "Access Control Policy
- "Incident Response Plan"
- "Disaster Recovery Plan"
- "Change Control Policy"

[63] All 14 physicians provided the same policies to me; all 14 indicated they have adopted the "Babylon Policies – Canada" policies provided to them by Babylon. The employment agreement and self-employed consultancy agreement between the physicians and Babylon state that the physicians are required to follow Babylon's policies.

[64] I also asked Babylon to provide the most current versions of its privacy and security policies and procedures. Babylon provided me with the following documents:

- "Babylon by Telus Health Privacy Policy"
- "Global ISMS Framework (BAB.POL.029)"
- "Global Information Governance Policy (BAB.POL.030)"
- "Information Security Policy (BAB.POL.032)"

- "Business Management System Roles and Responsibilities (BAB.POL.034A)"
- "Global Access Control Policy (BAB.POL.038)"
- "Global Network Security Policy (BAB.POL.040)"
- "Global Acceptable Use Policy (BAB.POL.042)"
- "Global Information Classification Policy (BAB.POL.043)"
- "Global Incident Management Policy (BAB.POL.044)"
- "Mobile Computing and Teleworking Policy (BAB.POL.045)"
- "Global Records Retention and Disposal Policy (BAB.POL.046)"
- "Change Management Policy (BAB.POL.048)"
- "Supplier Management Policy (BAB.POL.064)"
- "Global Operational Security Policy (BAB.POL.065)"
- "Business Continuity and Disaster Recovery Plan (BAB.POL.066)"
- "Global Data Protection Policy (BAB.POL.073)"
- "Whistleblowing Policy (BAB.POL.075)"
- "Physical and Environmental Security Policy (BAB.POL.078)"
- "Starters, Internal Mobility and Leavers Policy (BAB.POL.847)"
- "Disciplinary Policy (BAB.POL.850)"
- "Global Asset Management Policy (BAB.POL.851)"
- "Supplier Selection, Evaluation and Monitoring Procedure (BAB.POL.100)"
- "BAB.PRO.917_Visitor Procedures"
- "Babylon by Telus Health Clinic- Privacy Statement"
- "Babylon by Telus Health Technical Incident Escalation SOP (CAN-021)"
- "Babylon by Telus Health Records and Retention SOP (CAN-034)"
- "Babylon by Telus Health Request for Access to Patient Data (CAN-049)"
- "Babylon by Telus Health Privacy Office- Breach Assessment, Notification and Reporting (CAN-SOP-050)"
- "Copy of GP Video Consult Opening Script"
- "Babylon Health Canada Work from Home Policy"
- "Data Protection Impact Assessment Procedure"

[65] I reviewed the policies provided to me by the physicians and Babylon to assess whether they "facilitate the implementation of [HIA] and the regulations", as required by section 63 of HIA. As part of my review, I compared each of the privacy policies against the requirements outlined in the *Privacy Impact Assessment Requirements* document published by the OIPC.[10] This document includes a table identifying "General Privacy Policies" custodians should consider in order to meet their requirements under section 63 of HIA. Custodians are not required to implement exactly the policies identified in the table, but they should ensure their policies and procedures address the topics and issues described.

[10] Office of the Information and Privacy Commissioner of Alberta, "Privacy Impact Assessment Requirements", 2010.

Privacy Accountability Policy

[66] The Privacy Accountability Policy provided to me by the physicians says:

> Babylon Health's senior management plays an active role in decision-making related to privacy.
>
> Our Data Protection Officer (DPO) relates to Senior Management for relevant decisions. On a day-to-day basis, the Medical Director, the DPO and the Compliance Team are primarily responsible for managing compliance and adherence to the organization's privacy policies. Senior Management is notified and involved as relevant when escalation or specific approval is necessary. Any issues or major decisions are also reported and presented by the DPO at Management Review (Integrated Governance Committee). Privacy policies are developed by our legal team, the DPO and the Compliance team. All policies are reviewed annually to ensure they are up to date with current privacy legislation and reflect any changes. Updated policies are shared with employees by email and uploaded to a shared drive for reference. Where relevant, our Legal team engages external specialist resources to assist in policy development. Any changes to our current systems or services are considered circumstances that would require Babylon to conduct a privacy impact assessment. Our DPO, along with the medical director, are responsible for conducting the PIAs.

[67] I compared this policy against the OIPC's *Privacy Impact Assessment Requirements,* which identify the various elements that should be included in a policy addressing "Privacy Accountability".

[68] I found that the Privacy Accountability Policy provided by the physicians contains information regarding the organizational structure and accountability for privacy within Babylon, including responsibilities related to compliance, privacy policy development and privacy impact assessments (PIAs); however, the policy does not:

- Identify who is responsible for information security
- Include any commitment to protect confidentiality and to collect, use and disclose health information in a limited manner
- Include any commitment to maintain accuracy of health information
- Include any commitment to provide privacy training and awareness to employees
- Include any commitment to maintain technical and administrative safeguards to protect health information
- Address individuals' right to access health information and request corrections

[69] Although the Privacy Accountability Policy contains information regarding who is responsible for conducting PIAs within Babylon, there was no additional information regarding the specific circumstances that trigger a PIA, how frequently PIAs are reviewed, or what the physicians' role is in PIA development and submission to the OIPC.

[70] Perhaps most importantly, the policy does not address, or even reference, the role of the physicians with respect to privacy accountability, or their legal responsibilities under HIA.

Training Policy

[71] The Training Policy provided by the physicians includes information related to who receives training and by what method. Although the policy states that the training modules are updated semi-annually to reflect changes, it does not explicitly state whether all employees are required to review the training module on a regular basis. Further, the policy does not include information regarding sanctions that may result from non-compliance with the policies, which is a key component of a custodian's Training, Awareness & Sanctions policy, as outlined in the *Privacy Impact Assessment Requirements* document.

[72] The physicians did not provide any privacy and security training materials for my review; however, Babylon provided me with its Information and Cyber Security training and Information Governance training materials. Babylon says it provides these materials to all employees, including physicians and Babylon employees that provide administrative and clinical services for the physicians for the provision of health services.

[73] The Information Governance training addresses the principles of information security, confidentiality and data protection, data quality and integrity, data minimization, and purpose limitation. Although the training references compliance with various privacy regulations, there is no specific reference to Alberta or HIA. There is also no specific reference to HIA requirements regarding access and correction requests, expressed wishes and breach notification. Instead, there is a clear emphasis on European law, such as the guidance provided to employees that states, "If a UK member wants to exercise their privacy rights under the [*General Data Protection Regulation*]".

[74] The Information Governance training also states that Babylon employees shall review Babylon's policies, and the following in particular:

> **Data Protection Policy** (general overview of data protection obligations)
> **Data Subjects Rights Guidance** (what rights individuals have)
> **Information Security Policy** (policy on ensuring confidentiality, integrity and availability of information at Babylon)
> **Information Classification Policy** (how information is classified and handled at Babylon)
> **Access Control Policy** (how access to Babylon's assets are controlled)
> **Asset Management Policy** (how individual Information Technology and information assets are identified, categorised, classified and recorded)

[75] There is no clear alignment between these policies referenced in the Information Governance training and the "Babylon Policies – Canada" that were provided to me by the physicians. In addition, there is no indication that the physicians have access to, or are bound by, the policies identified in the Information Governance training.

[76] The Information and Cyber Security training materials address the principles of information security, confidentiality, data quality and integrity and data availability. Although they include requirements to comply with certain regulations, they do not

specifically reference HIA or the duty of custodians to protect health information per section 60(1). Instead, the materials include a listing of specific regulations, such as the European Union's *General Data Protection Regulation* (GDPR), USA's *Health Insurance Portability and Accountability Act* (HIPPA) and Singapore's *Personal Data Protection Act*.

[77] When I asked Babylon whether training provided to Alberta physicians and any Babylon employee who has access to Albertans' health information also includes training related to HIA, Babylon said:

> Babylon employees must complete Information and Cyber Security and Information Governance training. GDPR training was mandatory, but was recently replaced with Information Governance training to ensure applicability, relevancy and engagement in Canada.
>
> While our training is focused on key privacy principles and does not specifically [relate] to the Health Information Act, our privacy and data protection policies and procedures do address privacy requirements in respect of health information.

[78] In my view, training materials that refer to regulations that apply in jurisdictions other than Alberta may be misleading, as employees who are affiliates of the physicians may not realize that their activities related to the health services they provide in Alberta are, in fact, bound by HIA and not any of the regulations referenced in the training.

[79] This is particularly important since the Babylon employees who provide clinical and administrative services to the physicians are located in British Columbia and Ontario. The training materials direct Babylon associates to review the policies available. The listing of policies involved in the training consists of various frameworks and related policies. There is no indication of any Canada or Alberta-specific policies within the listing and the framework and policy documents listed do not align with the policies provided to me by the physicians.

Research Policy

[80] The Research Policy provided by the physicians contains references to HIA as well as the process that Babylon follows when it receives and processes research requests.

[81] The policy does not indicate how the physicians are notified of research requests or how they are involved in any such requests. The policy also does not indicate whether the physicians have delegated the responsibility for dealing with research requests to Babylon.

Monitoring and Auditing Policy

[82] The Monitoring and Audit Policy provided to me by the physicians addresses the following key points:

- Babylon monitors compliance with its privacy policies through a variety of measures

- The Canadian Medical Director has direct responsibility for ensuring that Babylon complies with HIA, as do managers/executives in respect of the data processing that takes place within their area of responsibility
- Compliance with the legislation is the responsibility of all employees/staff of Babylon who process personal data
- Data protection impact assessments are carried out in relation to the processing of personal data, and in relation to processing undertaken by other organizations on behalf of Babylon
- Babylon has a robust process for identifying and reporting data breaches

[83] Although the policy assigns accountability and responsibility for compliance with HIA, it does not describe the physicians' role in ensuring that their affiliates comply with HIA or the physicians' privacy policies. In addition, a key component of an effective monitoring and auditing policy is establishing and defining the requirement for affiliates to comply with the requirements of HIA, with respect to access to health information. This includes proactive monitoring for misuse of access to electronic records containing health information. This policy states that there is a robust process for identifying and reporting data breaches, but provides no clear information describing what is monitored to ensure compliance, the frequency of reviews and triggers for a formal audit, or review or activation of the physicians' incident response policy.

Data Access Request Policy

[84] The Data Access Request Policy assigns responsibility for handling correction requests to the Babylon Clinical Operations team. It provides information about the timelines for handling correction requests and the general process by which a correction request is handled, including the statement that the "data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement."

[85] The policy does not use HIA terminology (for example, it uses the term "data subject", which is not a term used within HIA). In addition, there is no indication of what process the physicians have implemented to address requests for access to health information by individuals or any fees associated with such requests. Moreover, the policy does not identify the physicians' role in handling access or correction requests. Despite the fact that the policy is entitled "Data Access Request Policy" there is no information related to the process by which the physicians or Babylon as the physicians' affiliate handle access requests they receive from individuals.

Third Party Policy

[86] The Third Party Policy is not directly relevant to the physicians' role of providing health services. Rather, it provides information regarding Babylon's process for engaging the services of third parties, including contractual arrangements, risk assessments and security requirements. There is no indication within this policy what, if any, the

physicians' roles or responsibilities are related to third parties or third party risk assessments.

Records, Retention and Disposal Policy

[87] The Records, Retention and Disposal Policy contains information related to the steps taken by Babylon during the course of handling patients' health information. It does not address the retention of health information after a physician has left Babylon, and it does not include statements regarding the physicians' responsibilities related to records, retention and the disposal of health information.

Information Classification and Handling Policy

[88] The contents of this policy are limited and the policy itself only contains three short sentences. It states:

> All personal identifiable information whether PHI or not is classified and handled as confidential. Proprietary information regarding processing is classified as restricted. Unclassified information is treated as "public".

[89] The policy uses the term "PHI", rather than the HIA definition of "health information". It states that all personal identifiable information, including PHI, is classified and handled as confidential. There is key information missing from this policy, including how the physicians classify health information and how information under each classification must be handled.

Risk Assessment and Treatment Policy

[90] The Risk Assessment and Treatment Policy emphasizes risks that are of strategic and operational importance to Babylon. While the policy notes there is a risk when "the confidentiality, integrity and availability of information is not reliable", there is no specific reference to health information or HIA within the policy. Although the policy states that Babylon reviews risks annually, as well as regularly, to ensure that they remain current and that the applied controls remain valid, there is no indication as to what the physicians' role is related to risk assessments or associated risk treatments.

Network and Security Policy

[91] Like the Third Party Policy, the Network and Security Policy is primarily a Babylon organizational-related policy. It provides some information related to the steps Babylon has taken to secure confidential information, including responsibilities around technical and physical security.

[92] The policy does not directly refer to health information or HIA. Although the policy provides guidance for Babylon employees, with regard to physical security measures used to safeguard confidential information, as well as the recommendation for

employees to store information on Babylon's network servers to prevent data loss, it is not clear how this guidance applies to the physicians.

Access Control Policy

[93] The Access Control Policy "defines the requirements of the company to ensure that access to information assets is authorised and subject to identification and authentication controls on the basis of business and security requirements". The policy "shall apply to all staff (permanent, temporary and contract) who have access to the company's information assets, including remote access".

[94] While this policy addresses user access management, including the assignment of a unique user ID as well as references to detailed processes that will be followed for terminating, modifying or revoking a user's access when the employee leaves Babylon, it does not include supplemental information, such as related processes that identify an employee's responsibilities or steps they must take related to access to health information.

Incident Response Plan

[95] Section 60.1 of HIA requires custodians to give notice of any loss or unauthorized access to or disclosure of individually identifying health information if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure. The notice must be given to:

- The Commissioner,
- The Minister of Health, and
- The individual(s) who is the subject of the health information.

[96] Accordingly, a breach (or incident) response policy/procedure is a key component of a custodian's policies and procedures to facilitate implementation of HIA.

[97] The physicians in this case provided me with an Incident Response Plan as part of the suite of "Babylon Policies – Canada". The Incident Response Plan identifies steps that are taken by Babylon to respond to privacy and security incidents. The policy uses terminology such as "data subject", "personal data" and "supervisory authority", which are not HIA terms for health information under HIA.

[98] Although the policy states that "privacy and security incidents must be reported immediately" to "the supervisory authority", it is not clear whether the supervisory authority means the Commissioner and the Minister as required by section 60.1(3) of HIA.

[99] The policy also says that "if the personal data breach is likely to result in high risk to the rights and freedoms of the data subject, Babylon notifies the data subjects

immediately". This statement does not acknowledge the requirements of section 60.1(2) of HIA, in which the threshold that triggers breach reporting/notification is "if there is a risk of harm to an individual as a result of the loss or unauthorized access or disclosure".

[100] Babylon also provided me with a document entitled "Babylon by Telus Health Privacy Office - Breach Assessment, Notification and Reporting (CAN-SOP-050)". This document contains the following provisions for reporting a breach:

> Where the Babylon Health Canada Privacy Officer (with guidance from the Legal Department) assesses a breach of personal information has resulted in a real risk of significant harm to an individual or individuals, Babylon Health Canada will, as required under the applicable legislation, notify other parties, such as but not limited to:
>
> - the individual whose information has been breached
> - the applicable privacy commissioner
> - a government minister
> - third parties that can help mitigate the risk to the individual such as law enforcement authorities and/or the Canadian Medical Protective Association
> - professional regulatory bodies (such as the College of Physicians and Surgeons)
> - other groups based on legal, professional, or contractual obligations
>
> Such notifications will be made as soon as possible.

[101] I note that this policy refers to a breach that "has resulted in a real risk of significant harm to an individual or individuals", rather than the lower "risk of harm" threshold in HIA. In addition, the policy does not refer to the HIA provisions that require custodians to consider all factors prescribed by the HIA Regulation in assessing whether there is a risk of harm to an individual.

Disaster Recovery Plan

[102] The Disaster Recovery Plan outlines steps Babylon takes to ensure the availability of the Babylon application and its infrastructure. Although it plays an important role in the physicians' understanding of Babylon's role with respect to these activities, it is more of an informational briefing rather than a policy that is directly related to the physicians' role in providing health services. In addition, the plan does not refer to health information or HIA, and does not address the responsibilities or obligations of the physicians.

Change Control Policy

[103] Similar to the Disaster Recovery Plan, the Change Control Policy functions as more of an informational briefing for the physicians to understand what steps Babylon takes to control any updates to its in-house developed software used within Babylon medical device software products. The policy does not directly relate to the physicians or how the physicians provide health services to patients within Alberta.

Summary

[104] Section 63 of HIA requires that custodians "establish or adopt policies and procedures that will facilitate the implementation of [HIA] and the regulations".

[105] My review identified significant gaps in the policies the physicians provided to me. I note, in particular, the physicians did not provide any policies respecting the collection, use and disclosure of health information, including how individuals are notified of the purpose(s) for which health information is collected, or how disclosure is handled by the physicians or on behalf of the physicians by Babylon.

[106] More significantly, the policies the physicians provided for the most part do not address or reference the role and legal responsibilities of the physicians as custodians subject to HIA, and do not refer to health information or HIA. It is also not clear when the policies came into effect, their review cycle, whether they are approved or by whom.

[107] Similarly, the policies provided to me by Babylon do not contain relevant information related to who approved them or when, or the date the policies came into effect. In some cases, such as with the breach response and access control policies, the content and wording differs from the policies the physicians provided to me.

[108] As with the policies provided by the physicians, I noted that many of the privacy and security policies provided by Babylon do not reference HIA, although they do reference other laws or regulations, such as GDPR. One exception is Babylon's Acceptable Use Policy, which references HIA and PIPA. However, since the physicians did not include the Acceptable Use Policy in the suite of "Babylon Policies – Canada" they provided to me, I am unable to determine whether they have reviewed or agreed to its contents.

[109] Overall, there is no indication that the physicians are even aware of or bound to the global and local policies provided to me by Babylon.

[110] In response to these concerns, Babylon and the physicians said:

> In their contract with Babylon, each physician accepted and agreed to be bound by Babylon's entire suite of privacy and information security policies and procedures. These policies and procedures address the key privacy and information security requirements of the HIA. The comments that the OIPC has made in respect of the policies are technical in nature and reflect unique structural requirements of the HIA. They do not relate in any way to key substantive privacy and information security controls.

[111] Babylon and the physicians also said my comments…

> …do not make any distinction between what is expressly required under the HIA and what is recommended by the OIPC, whether as per its written guidance or otherwise. As such, many of the findings should be presented as recommendations (which have largely been accepted and addressed as set out in the adjacent columns). It cannot be said that these technical issues result in complete non-compliance with section 63 of the HIA.

[112] Despite this submission, I maintain my findings. A key component of HIA, as outlined in section 63, is that custodians must establish or adopt policies and procedures that will **facilitate adoption of HIA and the regulations**. While the policies provided to me by the physicians and Babylon generally address privacy and security requirements, they do not facilitate implementation of the specific requirements of HIA and, in particular, they do not address or reference the role and legal responsibilities of the physicians as custodians subject to HIA.

[113] In addition, I found:

- There were significant gaps in the privacy and security policies provided to me by the physicians at the time of the investigation
- There were inconsistencies in the policies listed in the training provided to the physicians by Babylon, the policies provided to me directly by Babylon and the policies provided to me by the physicians

Finding

- The custodians (physicians) have not met the requirement of section 63 of HIA to establish or adopt policies and procedures that will facilitate the implementation of HIA and the regulations.

Recommendation

- I recommend that the physicians review and update all policies to include relevant approvals and effective date as well as ensure that all privacy policies developed by Babylon and adopted by the physicians clearly outline the responsibilities of the physicians and their affiliates under HIA.

Issue 2: With respect to services provided under employment/contract with Babylon, have the custodians (physicians) prepared privacy impact assessments as required by section 64 of HIA?

[114] Section 64 of HIA says:

> 64(1) Each **custodian must prepare a privacy impact assessment** that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information may affect the privacy of the individual who is the subject of the information.
>
> (2) The custodian **must submit the privacy impact assessment to the Commissioner for review** and comment **before implementing** any proposed new practice or system described in subsection (1) or any proposed change to existing practices and systems described in subsection (1). [emphasis added]

[115] Preparing a privacy impact assessment (PIA) is a key due diligence exercise by which custodians identify and address potential privacy risks associated with the collection, use and disclosure of health information. Through the PIA process, custodians have an opportunity to analyze potential impacts to privacy and consider reasonable security and privacy measures to mitigate these impacts. If done in a comprehensive manner and if controls are implemented, PIAs can help demonstrate that a custodian has complied with HIA's requirement to implement reasonable safeguards. Furthermore, by identifying and addressing risks in a reasonable manner, custodians may also reduce their risk of breaches related to health information.

[116] As previously noted, the OIPC received three PIAs related to Babylon:

- Case File #012533: PIA submitted by Dr. Keir Peterson, Medical Director of Babylon Health Canada Limited, for the Babylon by TELUS Health – Business to Business (B2B) product (submitted May 22, 2019)
- Case File #013187: PIA submitted by Dr. Keir Peterson regarding Babylon's "implementation of Netcare" (submitted June 18, 2019)
- Case File #015535: PIA submitted by Dr. Renie Traiforos, Alberta Physician Lead for Babylon, for the Babylon by TELUS Health – Business to Consumer (B2C) product (submitted March 16, 2020)

[117] I asked the 14 physicians, "In respect of your arrangement with Babylon Health Canada Ltd. have you prepared – or, reviewed and signed off on – a privacy impact assessment for the use and implementation of the system? If so, please provide applicable dates and indicate of this PIA was submitted to the Commissioner for review".

[118] I received letters from all 14 physicians that included the statement:

> I have reviewed and agree with the above-noted Privacy Impact Assessment and wish to participate. I endorse submissions made to date and delegate Dr. Keir Peterson, Medical Director, Babylon Canada as Lead Custodian for this initiative.

[119] The physicians signed the letters in August 2020; the letters were not in place in April 2020, when this investigation was initiated. At the time the PIAs were submitted, there was no indication that any of the 14 physicians (or any other physicians other than the Medical Director and Alberta Physician Lead) had reviewed, agreed to or endorsed the content.

Finding

- The custodians (physicians) have not met the requirement of section 64 of HIA to prepare and submit a privacy impact assessment prior to adopting the Babylon application to provide health services.

Recommendation

- I recommend that the physicians prepare and submit a privacy impact assessment that follows the requirements outlined in the *Privacy Impact Assessment Requirements* document, to the OIPC. In addition, all physicians in the future should have to review and sign-off on the PIA as part of their employment terms with Babylon.

Issue 3: With respect to services provided under employment or contract with Babylon, have the custodians (physicians) entered into agreement(s) with an information manager, as required by section 66 of HIA and 7.2 of the *Health Information Regulation*?

[120] As previously noted, Babylon provides information management and information technology services to the physician custodians, and qualifies as an information manager as defined in section 66(1) of HIA.

[121] Pursuant to section 66(2) of HIA, custodians are required to "enter into a written agreement with an information manager" (section 66(2)).

[122] A custodian that has entered into an agreement with an information manager "may provide health information to the information manager without the consent of the individuals who are the subjects of the information" (section 66(3)). The custodian, however, continues to be responsible for complying with HIA and the HIA Regulation in respect of information provided to the information manager.

[123] An information manager agreement (IMA) must meet the requirements set out in section 7.2 of the HIA Regulation, which says:

> 7.2 For the purposes of section 66(2) of the Act, an agreement between a custodian and an information manager must
>
> (a) identify the objectives of the agreement and the principles to guide the agreement,
> (b) indicate whether or not the information manager is permitted to collect health information from any other custodian or from a person and, if so, describe that health information and the purpose for which it may be collected,
> (c) indicate whether or not the information manager may use health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be used,
> (d) indicate whether or not the information manager may disclose health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be disclosed,
> (e) describe the process for the information manager to respond to access requests under Part 2 of the Act or, if the information manager is not to respond to access requests, describe the process for referring access requests for health information to the custodian itself,
> (f) describe the process for the information manager to respond to requests to amend or correct health information under Part 2 of the Act or, if the information manager is not to respond to requests to amend or correct health information, describe the process for referring access requests to amend or correct health information to the custodian itself,
> (g) describe how health information provided to the information manager is to be protected, managed, returned or destroyed in accordance with the Act,
> (h) describe how the information manager is to address an expressed wish of an individual relating to the disclosure of that individual's health information or, if the information manager is not to address an expressed wish of an individual relating to the disclosure of that individual's health information, describe the process for referring these requests to the custodian itself, and
> (i) set out how an agreement can be terminated.

[124] At the time this investigation was launched, 12 physicians were providing health services as employees of Babylon and two were providing services as self-employed consultants. Based on their role, the physicians signed either an employment agreement or a self-employed consultancy agreement.

[125] I reviewed copies of the templates for the employment contract as well as the self-employed consultancy agreement in place with the physicians. I also requested the individual, signed contracts from the physicians. Babylon did not assert that these agreements were intended to constitute IMAs; however, I reviewed these agreements against the requirements set out in section 7.2 of the Regulation, as they were provided to me as the only agreements that were in place between the physicians and Babylon, at the time the investigation was launched.

Employment Agreement

[126] The table below sets out the provisions of the Employment Agreement against the legal requirements of section 7.2 of the HIA Regulation.

Section 7.2 Requirement	***Employment Agreement***
(a) identify the objectives of the agreement and the principles to guide the agreement,	Not addressed
(b) indicate whether or not the information manager is permitted to collect health information from any other custodian or from a person and, if so, describe that health information and the purpose for which it may be collected,	Not addressed
(c) indicate whether or not the information manager may use health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be used,	Not addressed
(d) indicate whether or not the information manager may disclose health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be disclosed,	Not addressed
(e) describe the process for the information manager to respond to access requests under Part 2 of the Act or, if the information manager is not to respond to access requests, describe the process for referring access requests for health information to the custodian itself,	Not addressed
(f) describe the process for the information manager to respond to requests to amend or correct health information under Part 2 of the Act or, if the information manager is not to respond to requests to amend or correct health information, describe the process for referring access requests to amend or correct health information to the custodian itself,	Not addressed

Section 7.2 Requirement	*Employment Agreement*
(g) describe how health information provided to the information manager is to be protected, managed, returned or destroyed in accordance with the Act,	The "Termination of Employment" section says: Upon termination of your employment with the Company, you are required to immediately return to the Company all company documents, files, manuals, books, software, equipment, keys, identification or credit cards, and all other property belonging to the Company in your possession or control, including any electronic or other copies you may have ever made thereof.
(h) describe how the information manager is to address an expressed wish of an individual relating to the disclosure of that individual's health information or, if the information manager is not to address an expressed wish of an individual relating to the disclosure of that individual's health information, describe the process for referring these requests to the custodian itself, and	Not addressed
(i) set out how an agreement can be terminated.	Not addressed

[127] The Employment Agreement that 12 of the 14 physicians signed contains little to no explanation of what their responsibilities are related to the health information collected, used or disclosed by the physicians in their role with Babylon, or by Babylon in its role as information manager to the physicians.

[128] With respect to the legal requirements of an information manager agreement set out in section 7.2 of the *Health Information Regulation*, the only requirement that is even (partially) mentioned in the employment agreement is the requirement to "describe how health information provided to the information manager is to be ...returned or destroyed in accordance with the Act returned or destroyed in accordance with the Act" However, this provision of the agreement only requires the physician to return "company documents" to Babylon.

Family Physician Self Employed Consultancy Agreement (Consultancy Agreement)

[129] Two of the physicians associated with Babylon are self-employed consultants. I reviewed the provisions of the Consultancy Agreement against the legal requirements of section 7.2 of the HIA Regulation.

[130] For purposes of the table below, the Consultancy Agreement includes the following definitions:

> **Client Property:** all documents, books, manuals, materials, records, correspondence, papers and information (on whatever media and wherever located) relating to the Business or affairs of the Client or Group Company or its or their clients, customers, patients and business contacts, and any equipment, keys, hardware or software provided for the Consultant's use by the Client during the Engagement, and any data or documents (including copies) produced, maintained or stored by the

Consultant on the Client or the Consultant's computer systems or other electronic equipment during the Engagement.

Confidential Information: information in whatever form (including without limitation, in written, oral, visual or electronic form or on any magnetic or optical disk or memory and wherever located) relating to the business, clients, customers, patients, products, affairs and finances of the Client or any Group Company for the time being confidential to the Client or any Group Company and trade secrets including, without limitation, technical data and know-how relating to the Business of the Client or of any Group Company or any of its or their suppliers, clients, patients, customers, agents, distributors, shareholders, management or business contacts, including in particular (by way of illustration only and without limitation) information regarding patients and any assessment or treatment of a patient and including (but not limited to) information that the Consultant creates, develops, receives or obtains in connection with this Engagement, whether or not such information (if in anything other than oral form) is marked confidential.

…

Personal Information: information about an identifiable individual that is disclosed or transferred to Consultant, or collected or compiled by Consultant: (a) under this agreement; or, (b) in connection with, or in the course of the performance of, the Services or Engagement.

Privacy Laws: all applicable privacy laws, including without limitation, the Personal Information Protection Act (Alberta), as amended or replaced, and the Health Information Act, as amended or replaced.

Section 7.2 Requirement	***Employment Agreement***
(a) identify the objectives of the agreement and the principles to guide the agreement,	Not addressed
(b) indicate whether or not the information manager is permitted to collect health information from any other custodian or from a person and, if so, describe that health information and the purpose for which it may be collected,	9.1 The Consultant shall: (a) comply with Privacy Law, all Client policies and procedures and applicable professional and regulatory requirements and codes of practice in relation to the collection, use, disclosure, storage, security and destruction of Personal Information and patient records under the agreement, including without limitation, Personal Information relating to any employee, worker, customer, client, patient, supplier or agent of the Client; (b) collect, use and disclose Personal Information only to the extent necessary to fulfill the Consultant's obligations under this agreement; … (d) not collect, use or disclose any Personal Information in such a way or manner that will cause the Client to violate, breach or infringe its obligations and duties under Privacy Law or its contracts with customers or clients; … (f) collect, use and disclose the Personal Information only to the extent, and in such a manner, as is

Section 7.2 Requirement	*Employment Agreement*
	necessary for the purposes of performing the Services and in accordance with the Client's express instructions and authority from time to time and shall not collect, use or disclose the Personal Information for any other purpose;
(c) indicate whether or not the information manager may use health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be used,	Not addressed
(d) indicate whether or not the information manager may disclose health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be disclosed,	Not addressed
(e) describe the process for the information manager to respond to access requests under Part 2 of the Act or, if the information manager is not to respond to access requests, describe the process for referring access requests for health information to the custodian itself,	9.3 If the Consultant receives a request from an individual for access to or correction of Personal Information, the Consultant shall: (a) notify the Client within 2 business days of receiving such a request; (b) provide the Client with full co-operation and assistance in relation to any request made by an individual for access to or correction of Personal Information; and (c) not disclose or modify the Personal Information other than at the instruction of the Client or as provided for in this agreement.
(f) describe the process for the information manager to respond to requests to amend or correct health information under Part 2 of the Act or, if the information manager is not to respond to requests to amend or correct health information, describe the process for referring access requests to amend or correct health information to the custodian itself,	9.1 The Consultant shall: (a) comply with Privacy Law, all Client policies and procedures and applicable professional and regulatory requirements and codes of practice in relation to the collection, use, disclosure, storage, security and destruction of Personal Information and patient records under the agreement, including without limitation, Personal Information relating to any employee, worker, customer, client, patient, supplier or agent of the Client; (b) collect, use and disclose Personal Information only to the extent necessary to fulfill the Consultant's obligations under this agreement; … (d) not collect, use or disclose any Personal Information in such a way or manner that will cause the Client to violate, breach or infringe its obligations and duties under Privacy Law or its contracts with customers or clients;

Section 7.2 Requirement	*Employment Agreement*
	… (f) collect, use and disclose the Personal Information only to the extent, and in such a manner, as is necessary for the purposes of performing the Services and in accordance with the Client's express instructions and authority from time to time and shall not collect, use or disclose the Personal Information for any other purpose;
(g) describe how health information provided to the information manager is to be protected, managed, returned or destroyed in accordance with the Act,	7.3 The Consultant acknowledges that all Client Property and other documents and material whatsoever (including those made or created by the Consultant) relating to the business of the Client or any Group Company (and any copies of the same), shall be and remain the property of the Client or Group Company. 7.4 At any stage during the Engagement, the Consultant will promptly on request return all and any Client Property in their possession to the Client. **…** 9.1 The Consultant shall: (a) comply with Privacy Law, all Client policies and procedures and applicable professional and regulatory requirements and codes of practice in relation to the collection, use, disclosure, storage, security and destruction of Personal Information and patient records under the agreement, including without limitation, Personal Information relating to any employee, worker, customer, client, patient, supplier or agent of the Client; (b) collect, use and disclose Personal Information only to the extent necessary to fulfill the Consultant's obligations under this agreement; (c) implement and maintain appropriate physical, technical and organizational security measures to protect Personal Information against unauthorized access, collection, use, disclosure, loss or theft, and promptly upon request provide the Client with information about, and permit the Client to inspect and review, the Consultant's security measures with respect to Personal Information; (d) not collect, use or disclose any Personal Information in such a way or manner that will cause

Section 7.2 Requirement	*Employment Agreement*
	the Client to violate, breach or infringe its obligations and duties under Privacy Law or its contracts with customers or clients; (e) ensure that all Personal Information that the Consultant has processed during the provision of the Services is returned to the Client and that no Personal Information is retained by the Consultant after the Termination Date; (f) collect, use and disclose the Personal Information only to the extent, and in such a manner, as is necessary for the purposes of performing the Services and in accordance with the Client's express instructions and authority from time to time and shall not collect, use or disclose the Personal Information for any other purpose; (g) promptly comply with any request from the Client requiring the Consultant to amend, transfer or delete the Personal Information; (h) provide, at the Client's request, a copy of all Personal Information held by them in the format and on the media reasonably specified by the Client; (i) not transfer the Personal Information outside Alberta, Canada without the prior written consent of the Client; and (j) promptly inform the Client if any Personal Information is lost or destroyed or becomes damaged, corrupted, or unusable. The Consultant will restore such Personal Information at the Consultant's own expense. … 9.4 The Consultant shall notify the Client immediately if the Consultant becomes aware of any actual or suspected security breach related to Personal Information, including without limitation, any unauthorized access, use, disclosure, loss or theft of Personal Information, and cooperate with the Client in investigating and responding to such breach ... 12.2 On the Termination Date the Consultant shall:

Section 7.2 Requirement	*Employment Agreement*
	(a) immediately deliver to the Client all Client Property and original Confidential Information in their possession or under their control; (b) irretrievably delete any information relating to the Business of the Client or any Group Company stored on any magnetic or optical disk or memory and all matter derived from such sources which is in their possession or under their control outside the premises of the Client. For the avoidance of doubt, the contact details of business contacts or any information or date relating to clients or patients made during the Engagement are regarded as Confidential Information, and as such, must be deleted from personal social or professional networking accounts; and (c) provide a signed statement that they have complied fully with their obligations under this section 12, together with such evidence of compliance as the Client may reasonably request and confirmation that no copies or extracts have been retained by the Consultant on any media whatsoever.
(h) describe how the information manager is to address an expressed wish of an individual relating to the disclosure of that individual's health information or, if the information manager is not to address an expressed wish of an individual relating to the disclosure of that individual's health information, describe the process for referring these requests to the custodian itself, and	Not addressed
(i) set out how an agreement can be terminated.	11.1 Notwithstanding the provisions of section 2.2, the Client may terminate the Engagement with immediate effect with no liability to make any further payment to the Consultant (other than in respect of amounts accrued before the Termination Date) if at any time the Consultant [engages in or commits any of the acts set out in sub-clauses a through n]… 11.2 Subject to the requirements, prohibitions and limitations of the *Alberta Human Rights Act*, and any other governing and/or successor legislation thereto, the Client may deem this agreement to be frustrated and therefore terminated if the Consultant dies or becomes permanently incapacitated by accident or mental or physical illness which precludes the Consultant from performing the Services for an aggregate period of 28 days in any 52-week consecutive period.

[131] While the Consultancy Agreement references HIA and covers many of the topics set out in section 7.2 of the HIA Regulation, the provisions of the agreement assign ownership

of all health information to Babylon (the information manager) and, with respect to collection, use and disclosure of health information, bind the physicians (Consultant), and not the information manager (Babylon); that is, the provisions do not reflect the roles of custodian and information manager. Rather than describing Babylon's responsibilities related to its role as an information manager to the physician custodians, the agreement focuses on the prescribed requirements outlined by Babylon that the physicians must meet.

[132] The provisions of section 7.2 of the HIA Regulation outline what is required of an information manager. Given this, in my view the Consultancy Agreement does not meet the requirements set out in the Regulation. Custodians are responsible for the actions of their affiliates, including information managers, and not the reverse, as this agreement is written.

[133] Despite the fact that the Consultancy Agreement contains provisions related to the privacy and security of health information, I find that neither it nor the Employment Agreement meet the requirements set out in section 66 of HIA and section 7.2 of the HIA Regulation.

[134] Neither agreement adequately addresses the responsibilities of Babylon **in its role as information manager to the physicians**. The physicians are required to enter into an information manager agreement under section 66 of HIA. This is an important control whereby the physician custodians ensure control of patient health information when contracting with third parties to provide a health service. In my view, it is of significant concern that Babylon, the information manager, is dictating the terms of the agreements, despite the fact the custodians remain accountable to ensure the privacy and security of the health information at issue.

Finding

- With respect to services provided under employment/contract with Babylon, the custodians (physicians) have not entered into agreement(s) with an information manager, as required by section 66 of HIA and 7.2 of the *Health Information Regulation*.

Recommendation

- I recommend that the physicians enter into an information manager agreement with Babylon that meets the requirements of section 66 of HIA and 7.2 of the *Health Information Regulation*.

Issue 4: Have the custodians (physicians) met the requirements of section 8(4) of the *Health Information Regulation*, with respect to health information that is stored or used by a person in a jurisdiction outside Alberta?

[135] With respect to storing and using health information outside Alberta, section 8(4) of HIA Regulation sets out the various requirements that must be included in a written agreement with the party storing or using the health information.

[136] Section 8(4) of the HIA Regulation says:

> (4) In order to ensure the privacy and confidentiality of health information that is to be stored or used by a person in a jurisdiction outside Alberta or that is to be disclosed to a person in a jurisdiction outside Alberta, the custodian must, prior to the storage, use or disclosure of the information, enter into a written agreement with the person that
>
> (a) provides for the custodian to retain control over the health information,
> (b) adequately addresses the risks associated with the storage, use or disclosure of the health information,
> (c) requires the person to implement and maintain adequate safeguards for the security and protection of the health information,
> (d) allows the custodian to monitor compliance with the terms and conditions of the agreement, and
> (e) contains remedies to address any non-compliance with or breach of the terms and conditions of the agreement by the other person.
>
> (5) Subsection (4) does not apply to health information about an individual that is used in a jurisdiction outside Alberta solely for the purpose of providing continuing treatment and care to the individual.

[137] As part of my investigation, I asked all 14 physicians to "Please indicate where all health information collected, used, or disclosed through your use of the Babylon by TELUS Health app is maintained". I received identical responses from all 14 custodians. The responses included a table listing Babylon's third-party service providers along with the following associated information for each service provider:[11]

Type of Information	*Location Where the Information is Processed*
Credit card number, name, billing address	Canada
Imaging and lab results	Canada
Name, date of consultation, personal health number, billing code	Canada
Name, phone number, call recordings	Canada
IP address and device ID	Data is processed on the global Google infrastructure at the Google Cloud Platform locations.

[11] During the course of the investigation, I received various versions of tables that included information related to Babylon's third-party service providers. The information provided in each table varied slightly from the other tables.

Type of Information	*Location Where the Information is Processed*
IP address, device ID and location	Ireland
Postcode and IP address	Ireland
Audio call recordings	US
Consultation notes and prescriptions	US
Email, password and user ID	US
Government issued photo identification (e.g. driver's license, passport, identity card)	US
Name and email address	US
User ID	US
Video call recordings	US

[138] The responses provided to me by the physicians were provided to them by Babylon. The physicians submitted the responses and associated documentation after receiving my request for information. Based on the timing of the responses, the fact that the physicians had not endorsed any of the initial PIAs submitted by Babylon, and the coordinated response to my questions, I have no evidence or reason to believe that, at the time the initial investigation was launched, the physicians themselves were aware that health information they collect, use and store via consultations through the app is stored or used in jurisdictions outside Alberta via third party service providers engaged by Babylon UK, or disclosed to jurisdictions outside Alberta.

[139] When I asked Babylon about contracts or agreements that address the requirements of section 8(4) of the HIA Regulation, Babylon advised me, in part, as follows:

> Babylon uses a standard DPA (data processing agreement) with our service providers. While the language is a bit more GDPR focused, the spirit of this agreement is consistent with the requirements set out in S.8(4) which requires that:
>
> > *In order to ensure the privacy and confidentiality of health information that is to be stored or used by a person in a jurisdiction outside Alberta or that is to be disclosed to a person in a jurisdiction outside Alberta, the custodian must, prior to the storage, use or disclosure of the information, enter into a written agreement with the person that:*
> >
> > *(a) provides for the custodian to retain control over the health information;*
> > *(b) adequately addresses the risks associated with the storage, use or disclosure of the health information;*
> > *(c) requires the person to implement and maintain adequate safeguards for the security and protection of the health information;*
> > *(d) allows the custodian to monitor compliance with the terms and conditions of the agreement; and*
> > *(e) contains remedies to address any non-compliance with or breach of the terms and conditions of the agreement by the other person.*
>
> These agreements were in place prior to the IMAs and were entered into on behalf of the participating physicians by Babylon leadership. We have since appointed a Lead Custodian to enter into these agreements on behalf of Alberta physicians.

These [DPAs] outline:

- The data processor/data controller relationship to demonstrate Babylon's physicians have control over the information and instructs the service providers on processing;
- provisions around service providers providing information in the event a PIA is required;
- Babylon's ability to monitor adherence to the agreement;
- requirements for these service providers to have security measures in place at minimum equal to those found in Babylon's policies and procedures; and
- provisions if Babylon were to conduct an audit.

[140] I received and reviewed a number of agreements between Babylon and its third party service providers. However, in its response to my question regarding the requirements of section 8(4) of the HIA Regulation, Babylon highlighted a specific DPA as an example of a Data Processing Agreement that was in place between Babylon UK and its third party providers at the start of this investigation. I reviewed the agreement against the requirements set out in section 8(4) of the HIA Regulation. My findings are as follows:

Section 8(4) Requirement	***Data Processing Agreement Provision***
(a) provides for the custodian to retain control over the health information,	Not addressed
(b) adequately addresses the risks associated with the storage, use or disclosure of the health information,	2.2 [Third Party] shall comply with the requirements of the Data Protection Laws applicable to controllers in respect of the use of Merchant Data under this Agreement (including without limitation, by implementing and maintaining at all times all appropriate security measures in relation to the processing of Merchant Data and by maintaining a record of all processing activities carried out in respect of Merchant Data) and shall not knowingly do anything or permit anything to be done with respect to the Merchant Data which might lead to a breach by the Merchant of the Data Protection Laws.
(c) requires the person to implement and maintain adequate safeguards for the security and protection of the health information,	3.9 **Security.** [Third Party] shall, as a minimum, implement and maintain appropriate technical and organizational measures as described in Attachment 1, Appendix 2 of the Addendum to keep Customer Data secure and protect it against unauthorised or unlawful processing and accidental loss, destruction or damage in relations to the provision of the Services. Since [Third Party] provides the Services to all Merchants uniformly via a hosted, web-based application, all appropriate and then-current technical and organisational measures apply to [Third Party]'s entire customer base hosted out of the same data centre and subscribed to the same service. Merchant understands and agrees that the technical and organizational measures are subject to technical progress and development. In that regard, [Third

Section 8(4) Requirement	*Data Processing Agreement Provision*
	Party] is expressly permitted to implement adequate alternative measures as long as the security level of the measures is maintained in relation to the provision of the Services. In the event of any detrimental change [Third Party] shall provide a notification together with any necessary documentation to Merchant by email or publication on a website easily accessible by Merchant.
(d) allows the custodian to monitor compliance with the terms and conditions of the agreement, and	3.8 **Audits and Certifications.** Where requested by Merchant, subject to the confidentiality obligations set forth in the Agreement, [Third Party] shall make available to Merchant (or Merchant's independent, third-party auditor that is not a competitor of [Third Party] or any member of PayPal or the Paypal Group) information regarding [Third Party]'s compliance with the obligations set forth in this Addendum in the form of the third-party certifications and audits (if any) set forth in the Privacy Policy set out on our website. Merchant may contact [Third Party] in accordance with the "Notices" Section of the Agreement to request an on-site audit of the procedures relevant to the protection of personal data. Merchant shall reimburse [Third Party] for any time expended for any such on-site audit at [Third Party]'s then-current professional services rates, which shall be made available to Merchant upon request. Before the commencement of any such on-site audit, Merchant and [Third Party] shall mutually agree upon the scope, timing, and duration of the audit in addition to the reimbursement rate for which Merchant shall be responsible. All reimbursement rates shall be reasonable, taking into account the resources expended by [Third Party]. Merchant shall promptly notify [Third Party] with information regarding any non-compliance discovered during the course of an audit.
(e) contains remedies to address any non-compliance with or breach of the terms and conditions of the agreement by the other person.	Not addressed

[141] I found the sample DPA contained a number of provisions addressing the requirements set out in section 8(4) of the HIA Regulation with respect to health information that is stored or used in a jurisdiction outside Alberta, or disclosed to a person in a jurisdiction outside Alberta. However, notably, the DPA does not meet the requirements of sections 8(4)(a) and (e).

[142] I am particularly concerned that the sample DPA I reviewed does not provide for the custodians to retain control of health information as section 8(4)(a) of HIA explicitly requires. In fact, the custodians are not direct parties to the agreement; the DPAs have been entered into by Babylon UK and its third party service providers. Babylon UK is not a custodian. There is no evidence that the physicians authorized Babylon UK to enter into these agreements on their behalf. During the course of the investigation, the physicians gave me a copy of IMAs they entered into with Babylon, and with respect to subcontracting, the IMA states:

> We may disclose Data to External Providers to provide the Services and facilitate Babylon Providers' provision of Clinical Services to Patients, and otherwise in accordance with the Privacy Policy and any consents given by the Patient.
>
> We may transfer Data to our subcontractors, or provide our subcontractors with access to Data, to the extent necessary to assist us with the provision of Services provide such subcontractors are bound by obligations of confidentiality and information security in respect of the Data that are at least as restrictive as those imposed on us under this Agreement.

[143] In my view, the IMA describes services that Babylon may provide, but it does not demonstrate clear authority for Babylon leadership to sign agreements with their subcontractors on behalf of the physicians.

[144] In addition to the IMA, and during the course of the investigation, the physicians provided me with a copy of Information Sharing Agreements they entered into with Babylon. With regard to providing authority to enter into agreements on the physicians' behalf, the Information Sharing Agreement states:

> The purpose of this Information Sharing Agreement ("ISA") is to provide the terms upon which Physicians document and share patient Health Information in a physical and virtual clinic setting; and enable the access to, use of, and disclosure of Health Information with one another; to define and manage the permitted uses and disclosures of that Health Information; and to identify the authority granted to a Lead Clinic Custodian to sign documentation and enter into Agreements with third parties including Information Managers (as defined by the HIA) on behalf of the Physicians at BbTH.

[145] Despite the fact that the Information Sharing Agreement authorizes the Lead Clinic Custodian to enter into agreements with third parties, including information managers on behalf of the physicians, in my review of the various agreements between Babylon UK and its service providers, the Lead Clinic Custodian has not signed any of the agreements.

[146] Health information is used or stored in jurisdictions outside of Alberta by virtue of the data protection agreements that Babylon UK has in place with its third party service providers. These various agreements contain several of the provisions required by section 8(4) of the HIA Regulation; however, they do not meet sections 8(4)(a) and (e). Of particular concern is the fact that the agreements do not provide custodians with the ability to retain control of the health information. Moreover, the physicians are not direct parties to the agreements; the agreements are in place between Babylon UK and

their third-party service providers. Finally, there is no evidence that the physicians have authorized Babylon or Babylon UK to enter into these agreements on their behalf.

[147] Despite the fact that the physicians provided me with a third-party service provider table upon my request, there is no indication the physicians knew where health information was being used or stored prior to when I asked them.

[148] In response to these concerns, Babylon and the physicians said:

> … Babylon's Data Processing Agreements met the substantive requirements of section 8(4) of the Health Information Regulation. Further, it is unreasonable and unworkable to require physicians to review each contract with service providers. It is consistent with the accountability and other requirements of the HIA for physicians to instruct, authorize or generally delegate this responsibility and authority to an information manager, which physicians have done through IMAs as described in the adjacent columns.

[149] Despite these assertions, I maintain my finding that the custodian physicians have not met the requirements of section 8(4) of the *Health Information Regulation*, particularly with regard to the requirement to provide for the custodians to retain control over the health information.

Finding

- The custodians (physicians) have not met the requirements of section 8(4) of the *Health Information Regulation*, with respect to health information that is stored or used by a person in a jurisdiction outside Alberta.

Recommendation

- I recommend that the physicians review and revise existing agreements to ensure they meet the requirements of section 8(4) of the *Health Information Regulation*. In addition, the physicians should provide the OIPC with a copy of updated agreements as well as an updated PIA within six months from the date of this report.

Issue 5: Have the custodians (physicians) taken reasonable steps to maintain administrative and technical safeguards to protect health information as required by sections 60 and 63 of HIA, and section 8 of the *Health Information Regulation*?

[150] Custodians have a duty to protect health information in their custody or under their control. Section 60 of HIA states:

> 60(1) A custodian must take reasonable steps in accordance with the regulations to maintain administrative, technical and physical safeguards that will
>
> > (a) protect the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information…
> >
> > (c) protect against any reasonably anticipated …
> >
> > > (ii) unauthorized use, disclosure or modification of the health information or unauthorized access to the health information,
>
> (2) The safeguards to be maintained under subsection (1) must include appropriate measures
>
> > (a) for the security and confidentiality of records, which measures must address the risks associated with electronic health records

[151] Section 8 of the HIA Regulation sets out additional security requirements including:

> **Security of health information**
>
> 8(1) A custodian must identify, and maintain a written record of, all of its administrative, technical and physical safeguards in respect of health information.
>
> (2) A custodian must designate an individual who is responsible for the overall security and protection of health information in the custody or under the control of the custodian.
>
> (3) A custodian must periodically assess its administrative, technical and physical safeguards in respect of
>
> > (a) the confidentiality of health information that is in its custody or under its control and the privacy of the individuals who are the subjects of that information,
> > (b) any reasonably anticipated threat or hazard to the security or integrity of the health information or to the loss of the health information, and
> > (c) any unauthorized use, disclosure or modification of the health information or unauthorized access to the health information.

[152] These sections of HIA and the HIA Regulation require that custodians identify threats to patient privacy and confidentiality and take reasonable steps to maintain administrative, technical and physical safeguards that will mitigate identified risks, including the risks of unauthorized access to and use of health information.

[153] Further, HIA specifically requires that measures be taken to address the risks associated with electronic health records. Custodians are required to establish or adopt policies and procedures, and maintain a written record of the administrative, technical and physical safeguards that are implemented. This requirement extends to their affiliates, including information managers, insofar as their management of health information on behalf of the custodians.

[154] Custodians must ensure their affiliates are aware of and adhere to administrative, technical and physical safeguards that have been implemented. Finally, any collection, use or disclosure of health information by an affiliate of a custodian is considered to be collection, use or disclosure by the custodian.

[155] I considered the safeguards that the physicians had in place to meet these obligations under HIA. Given the specific matters at issue in this investigation, I focused on administrative and technical safeguards.

Administrative Safeguards

Policies and Procedures

[156] Earlier in this report, I reviewed and provided my analysis on the policies and procedures provided by the physicians and Babylon. I will not repeat that analysis here, but will reiterate my finding that the physicians contravened section 63 of HIA by failing to establish or adopt policies and procedures to facilitate the implementation of HIA and the regulations.

[157] I will, however, make further comments on the Access Control Policy provided to me by the physicians, as it is a key administrative safeguard.

[158] The Access Control Policy provided to me by the physicians states "password changes are enforced, re-use of passwords is prohibited and seven-character alphanumeric passwords are required". I note that this password strength and composition is considered weak by today's standards. It is a generally accepted industry standard that passwords should be, at a minimum, eight characters.[12] Weak passwords present a risk to the privacy of health information as they contribute to a greater ability for systems to be compromised with passwords that are easily guessed or cracked by brute force applications.

[159] In contrast, Babylon's Global Access Control Policy (BAB.POL.038) states that passwords must be a minimum of eight characters, containing at least one lowercase letter, one uppercase letter, one numeric character and one non-alphanumeric. In addition, the policy states that users sign a statement acknowledging their responsibility to keep

[12] See, for example, National Institute of Standards and Technology (NIST): U.S. Department of Commerce, "NIST Special Publication 800-63B: Digital Identity Guidelines", Appendix A, June 2017.

passwords confidential and users are made aware of the organization's password requirements.

[160] Based on the information provided to me by the physicians, I see no indication that they have been made aware of or agreed to the eight-character, complex password requirements set out in Babylon's Access Control Policy (BAB.POL.038). Given this inconsistency, it is not clear to me that that the physicians are aware of or enforce this important security measure.

[161] Also with respect to the Access Control Policy, I asked Babylon "who reviews access to Babylon to ensure that users have only accessed the health information they have the legal authority to access?"

[162] I requested documentation related to the audit process, "including but not limited to roles and responsibilities and frequency of reviews". Babylon responded:

> The scope of the Access Control Policy applies to Babylon employees "This Access Control Policy shall apply to all staff", and it is not meant to apply to patients. Internal employee access to systems is role based, based on pre-authorised role groups or personas. Activity logs for critical systems are monitored by Babylon's Managed Security Services Supplier (MSSP), with second line escalation to Babylon's Security Operations team. Monitoring policies and procedures are enclosed for the Commissioner's review. Babylon is currently rolling out a quarterly Privileged User Access Review (PUAR) program for critical systems.

[163] Babylon included a Log Management Standard Operating Procedure in its response, which focuses on system and technical issues and does not include a process for determining if access to health information is in accordance with a physician or employee's role.

[164] I previously found that the physicians contravened section 63 of HIA by failing to establish or adopt policies and procedures to facilitate the implementation of HIA and the regulations. Further to that previous discussion, the Access Control Policy, in particular, is inconsistent with Babylon's standards with respect to password security, and omits key information about determining if access to health information is in accordance with a physician or employee's role.

Privacy Awareness Training

[165] Privacy awareness training is an important administrative safeguard, as it provides the opportunity for custodians and their affiliates to understand their responsibilities under HIA. In addition, privacy awareness training assists with the understanding of the security safeguards and related best practices that should be used to reduce the likelihood of breaches of health information.

[166] It is the responsibility of the physicians, as custodians, to ensure their affiliates are aware of their responsibilities related to HIA. Affiliates of the physicians include

Babylon, and in particular the Babylon employees who provide clinical and administrative support for health services provided by physicians.

[167] Earlier in this report, I reviewed the Training Policy provided to me by the physicians, and the training materials provided to me by Babylon. I said that "training materials that refer to regulations that apply in jurisdictions other than Alberta may be misleading, as employees who are affiliates of the physicians may not realize that their activities related to the health services they provide are, in fact, bound by HIA and not any of the regulations referenced in the training". I also found that the list of policies found in the Babylon training materials did not align with the policy documents provided to me by the physicians.

[168] Given this, in my view, the physicians have not met their requirement to implement HIA-related privacy and security awareness training for their affiliates, as a key administrative safeguard.

Confidentiality Agreements

[169] Confidentiality agreements are another key administrative safeguard, and should clearly reflect the requirements under HIA related to confidentiality of health information.

[170] In this case, the physicians said that Babylon, as their affiliate, provides services that enable the physicians' use of the application. Babylon support staff assist with tasks, such as helping with troubleshooting, as well as "sending labs, investigations, referrals and prescriptions" to the intended recipients. As affiliates of the custodian physicians, these entities have access to health information, and are required to comply with the requirements set out in HIA and the regulations, and the policies and procedures established or adopted under section 63.

[171] I asked Babylon if employees sign confidentiality oaths at the time of hire and on an annual basis. Babylon said:

> In addition to relevant information protection policies at Babylon, employees are bound by confidentiality provisions within their employment contracts. An example of a confidentiality provision can be found within the Albertan physician contracts, an extract of which is below:
>
> 1. Confidential Information
>
> "Confidential Information" means trade secrets and other information, in whatever form or media, in the possession of the Company and owned by the Company or by any of its suppliers, clients or other business partners (collectively, "Associates"), which is not generally known to the public and has been specifically identified as confidential or proprietary by the Company or the Associate from whom the Company has obtained its rights, or by its nature is such that it would generally be considered confidential in the industry in which the Company operates, or which the Company is legally obligated to treat as confidential or proprietary. Confidential Information includes, without limitation, the Company's ideas, inventions, formulae, techniques, processes, know how, show how, trade secrets, designs, methods, specifications, plans, devices, financial statements and forecasts, client information, relationship with consultants and other Associates, contracts, business plans, budgets,

accounting information, documents/programs developed to manage the business costing and pricing methods, general company policies, training content and programs, and sales and marketing programs, plans and strategies.

You will have access to Confidential Information in the course of your employment with the Company. Both during and after your employment, you will maintain the confidentiality of the Confidential Information of the Company and will protect the Confidential Information from disclosure by exercising a standard of care as may reasonably be expected to preserve its secret and confidential nature. You will not, other than as reasonably required in the course of your employment and except as required by law, use, copy, reproduce, disclose, publish, make available, distribute or otherwise exploit the Confidential

Information, directly or indirectly, without first obtaining the written consent of the Company, including in respect of any product or service that is competitive with any of the products or services of the Company.

You acknowledge that irreparable harm may result to the Company if you breach your obligations under this provision and that such a breach may not properly be compensated by an award of damages. Accordingly, the remedy for any such breach may include, in addition to other available remedies and damages, injunctive relief or other equitable relief enjoining such breach at the earliest possible date.

[172] I also asked Babylon to provide copies of confidentiality agreements that are signed by Babylon employees who are **not physicians** but who provide support and therefore have access to health information. Babylon provided the master employment contract template for British Columbia and for Ontario, both of which contain confidentiality clauses. Babylon explained that since their only physical locations in Canada are in Vancouver and Toronto, the clinical support staff providing support to Alberta physicians are located in these two locations. As such, there is no Alberta employment agreement. The confidentiality clauses within the British Columbia contract are exactly the same as those in the Employment Agreement for physicians.

[173] The confidentiality clauses within the Ontario employment agreement read somewhat differently, and say:

As a consequence of performing the Services, you acknowledge that you have had and will continue to have access to and have been and will be entrusted with information about certain matters and things which are confidential to the Company, including, without limitation: trade secrets, lists of past, present and prospective clients, customers, employees, suppliers, business partners, and information related to such persons and entities (including without limitation, names, customer preferences, financial information, addresses or telephone numbers), financial data, operational procedures, product specifications, plans for future products and services, plans for growth, ideas, inventions, formulae, techniques, processes, know how, show how, trade secrets, designs, methods, specifications, devices, documents/programs developed to manage the business costing and pricing methods, general company policies, training content and programs, and sales and marketing programs, plans and strategies (collectively, the “Confidential Information”); and other information that is confidential to any person or other entity having dealings with the Company (the “Third Party Confidential Information").

All Confidential Information is the exclusive property of the Company. You will not, either during the Term or anytime thereafter, without obtaining written permission in advance from the Company,

> disclose or use for any purpose any Confidential Information or Third Party Confidential Information except to the extent required to perform the Services.
>
> This obligation will not apply with respect to information which:
>
> (a) at the time of its disclosure to you was or subsequently becomes (through no act or omission on your part) generally available to the public;
>
> (b) is received by you from a third party legally entitled to give such information to you, other than as a result of your employment with the Company,
>
> provided that in respect of such information you will remain obligated to act in the best interests of the Company.

[174] As stated previously, the Employment Agreement between Babylon and the physicians does not specifically reference health information or the requirements of HIA. In addition, the master employment contracts for non-physician employees in British Columbia and Ontario do not reference HIA, and do not explicitly include health information within the definition of "confidential information". Furthermore, there is no indication that confidentiality provisions must be adhered to and signed-off by Babylon staff – physician, non-physician or consultant – on a regular basis.

Technical Safeguards

[175] The physicians providing health services through the Babylon application do not directly administer the technical safeguards associated with the application; this is part of the service offering provided by Babylon to the physicians. Despite this, HIA makes the physicians responsible for ensuring appropriate technical safeguards are in place.

[176] A key component of a PIA is a risk assessment, which should contain a comprehensive listing of privacy and security risks and mitigating measures. Although Babylon submitted PIAs to the OIPC, the PIAs did not contain sufficient information regarding the technical controls that are in place to mitigate the risks to health information that Babylon identified in their included privacy risk assessment and mitigation plans.

[177] I previously found that, at the time the PIAs were submitted, there was no indication that any of the 14 physicians (or any other physicians other than the Medical Director and Alberta Physician Lead) had reviewed, agreed to or endorsed the content.

[178] The administrative safeguards adopted by the physicians, including policies and procedures, privacy and security awareness training, and confidentiality agreements, do not meet the standard of best practice that would be reasonably expected when dealing with health information.

[179] The PIAs submitted by Babylon did not include a thorough privacy and security risk assessment or mitigation table, and there is no indication the physicians reviewed, agreed to or endorsed the content.

[180] The lack of appropriate administrative safeguards, coupled with the failure to demonstrate that they were aware of the technical safeguards in place at the time of the initial investigation, leads me to find that the physicians did not meet the requirement of sections 60 and 63 of HIA or section 8 of the HIA Regulation.

[181] In response to these concerns, Babylon and the physicians stated the following, in part:

> [A]t the commencement of the investigation, Babylon had implemented a robust suite of privacy and information security policies designed to protect all personal information (including health information). The administrative and technical safeguards in place to protect personal information and health information met or exceeded the requirement to maintain reasonable and appropriate security measures. The tone of these findings suggests that there was a material risk to the safeguarding of personal information, which is simply not supported by any of the facts. The physicians reasonably relied on Babylon's information security program. It is entirely appropriate – if not ideal – for physicians to rely upon Babylon's technology and security expertise and in this way. Moreover, none of the specific recommendations outlined go to the core of privacy and information security risk management. Rather, the findings focus on technical issues raised by the specific structural requirements of the HIA, which are unique as compared with health privacy legislation across the rest of the country. The findings also appear to be largely based on a review of the information provided in the PIA, rather than an assessment of Babylon's actual information security and privacy controls, which are consistent with a number of internationally recognized information security standards.

[182] I considered this submission by Babylon and the physicians but nonetheless maintain my original findings and recommendations. Despite the assertion that "the findings focus on technical issues raised by the specific structural requirements of the HIA, which are unique as compared with health privacy legislation across the rest of the country", HIA is the legislation that applies in this case. In my view, the custodians have not established or adopted administrative safeguards – policies and procedures, training, and confidentiality agreements – that facilitate the implementation of HIA.

[183] While my investigation did not include a review of the technical safeguards that Babylon has in place, my analysis in this section is based on evidence provided that indicates that, at the time the investigation commenced, the physicians were not aware of and had not evaluated the safeguards Babylon had in place to protect health information. Safeguards were not fully described in the PIAs initially submitted by Babylon. Furthermore, the physicians had not endorsed the PIAs initially submitted to the OIPC. Therefore, I maintain my findings and recommendations as outlined above.

Finding

- The custodians (physicians) have not taken reasonable steps to maintain administrative and technical safeguards to protect health information as required by sections 60 and 63 of HIA, and Section 8 of the *Health Information Regulation*.

Recommendations

- I recommend that the physicians ensure that any privacy and security awareness training that is provided by Babylon and adopted by the physicians is updated to include references to HIA and its associated requirements.
- I recommend that the physicians ensure that privacy and security awareness training includes references to the policies that are provided to Alberta-based physicians.

Issue 6: Do the custodians (physicians) collect and use health information in a limited manner as required by section 58 of HIA?

[184] Section 58 of HIA requires custodians to collect, use and disclose only the amount of health information that is essential to enable the custodian, or the recipient of the information, to carry out the intended purpose. Section 58 reads as follows:

> 58(1) When collecting, using or disclosing health information, a custodian must, in addition to complying with section 57, collect, use or disclose only the amount of health information that is essential to enable the custodian or the recipient of the information, as the case may be, to carry out the intended purpose.

[185] I considered section 58 with respect to the physician custodians' collection and use of identification information and video or audio recordings in particular, as well as location information.

Government-Issued Identification and Selfie Photo

[186] When an individual downloads the Babylon by TELUS Health app to their mobile device, they are required to complete a registration process and create login credentials. Through the registration process, identifiers such as first and last name, email address, and physical address including postal code are collected.[13]

[187] Once registered and in the application, the individual is able to access Clinical Services. As noted previously, "Clinical Services" are described in Babylon's Terms and Conditions to include "remote video and voice consultations with our Practitioners".

[188] When Babylon's physicians (custodians) provide these services through the app, they collect and use "health information" as defined in section 1(1)(k) of HIA, including both "diagnostic, treatment and care information" as well as "registration information".

[189] "Diagnostic, treatment and care information" includes information about the physical and mental health of an individual, and a health service provided to an individual (section 1(1)(i)).

[190] "Registration information" includes:

> (i) demographic information, including the individual's personal health number;
> (ii) location information;
> (iii) telecommunications information;
> (iv) residency information;
> (v) health service eligibility information;
> (vi) billing information [section 1(1)(u) of HIA]

[13] The collection and use of this information is addressed in OIPC Investigation Report P2021-IR-02.

[191] In order to participate in "video and voice consultations" with the physicians, individuals must first book an appointment, which requires the individual to verify their identity by submitting two photographs: a selfie photograph and photo of government-issued identification, such as a driver's license, passport, national identity card or permanent residence card. Individuals are required to upload both images to the Babylon app. Babylon then transfers the images to a third-party service provider in order to validate the individual's identity.

[192] I asked Babylon to provide additional information regarding the collection and use of government-issued identification and selfie photographs. Babylon provided responses on more than one occasion, including the following statement, which was provided to me early in the investigation:

> Verifying patient identity in a telemedicine service is essential for patient care. Babylon requires a driver's license or other form of identity document (such as a passport, national identity card or residence permit card) in order to verify the identity of the patient. It is important that Babylon verifies identity to ensure that clinicians are treating, prescribing and diagnosing the right patient, and also for billing purposes. The identity document is retained for a maximum of 20 days (this can be reduced to 1 day).

[193] Babylon added to their response on a later date, stating:

> Babylon requires a driver's license or other form of identity document (such as a passport, national identity card or residence permit card) in order to verify the identity of the patient before an appointment with a physician is booked. A copy of this ID documentation is uploaded via the Babylon app along with a selfie of the patient. The identity document and selfie are then checked, matched and verified through use of technology, that confirms that the selfie photo matches the photo on the identity document and checks that the identity document is valid and current. The identity document is retained for one day.
>
> Appropriate and robust verification of patient ID is necessary in the context of the healthcare service being provided. Whereas in an in-person setting, a receptionist or clinician can see the patient, Babylon is not able to do this. Throughout the health-care industry, the failure to correctly identify patients continues to result in medication errors, transfusion errors, testing errors and wrong person procedures.
>
> Patients themselves may submit false information in order to access treatment not otherwise available to them. Incorrect patient identification at registration, could cause the patient record to be linked to the wrong records throughout their interaction with Babylon. Robust identification prevents duplicate and mismatched patient records. If there are too many duplicate records in the system, there is a risk of misidentification occurring when the search query by a physician returns multiple records with the same name or date of birth. The physician may not be able to find the correct record for the patient. Data integrity of medical records can be impacted.

[194] I agree that verifying a patient's identity is essential for patient care in order to reduce the likelihood of medical errors. Further, the HIA definition of "registration information" (a category of health information) includes "health services eligibility information" and "billing information".

[195] The same concerns apply when providing health services to patients in person. However, when health services are provided in person, individuals are **not** required to provide a copy of government-issued identification or a selfie photograph at the time of booking an appointment. Requiring app users to do so is, in my view, going beyond what is essential to achieve the custodian's purposes (verifying identity and eligibility to receive health services).

[196] Babylon provided further information explaining the rationale for collecting identification information, including the following:

> There is an increase in virtual health services, with clinical providers often relying on email, text or audio phone calls with patients for the provision of care. Risks of misidentification and therefore misdiagnosis and mistreatment can exist via these channels of communication with patients. Failure to appropriately verify patient identity can also lead to healthcare fraud. Babylon aims for a high standard of care, whereby physicians can consult with their patients through a video call, with the comfort of knowing that their identity has been assured prior to the commencement of an appointment.
>
> Too often, patient identification errors only receive their due attention after a serious error or incident occurs, such as one that results in patient harm. Technological advances and initiatives, as adopted by Babylon, can help to minimize this issue. Patient identification errors are preventable with the right technologies and safeguards in place.

[197] Based on the information provided to me, I am not satisfied that misidentification, medical error or fraud are more prevalent in a virtual setting.

[198] I note further that Babylon's submission says:

> A copy of this ID documentation is uploaded via the Babylon app along with a selfie of the patient. The identity document and selfie are then checked, matched and verified through use of technology, that confirms that the selfie photo matches the photo on the identity document and checks that the identity document is valid and current.

[199] From this, I understand Babylon is describing the use of a facial recognition technology, which raises additional concerns to the extent non-essential sensitive identification information is being collected through the app and transferred to a third party provider, outside of Alberta and Canada, where it is converted to a biometric and retained for anywhere from 1 to 20 days.[14]

[200] In my view, the physicians' purposes can be accomplished by asking the individual to show government-issued identification to the camera at the time of the consultation, as is commonly done with in-person consultations. In the event a consultation is by telephone, the individual could be asked to confirm certain pieces of information (date of birth) before proceeding, as is a common practice when providing financial services

[14] Babylon repeatedly objected to the use of the term "facial recognition technology" in this report. I have used this term to describe the use of a computer algorithm that compares the distinctive details about a person's face from one image to another.

by telephone. It is not essential that the physicians (through Babylon) collect copies of government-issued identification and a selfie photograph from individuals in order to carry out their purpose of verifying eligibility for health services and verifying identity in order to reduce the likelihood of medical errors.

[201] In my view, identity verification can be accomplished in ways that do not involve the collection of this information. Therefore, I find the physicians have collected and used more health information than essential to carry out intended purposes of verifying an individual's identity to prevent fraudulent use of health services and mismatched patient records.

[202] In response to this finding, Babylon and the physicians made an additional submission, emphasizing that "The identity of app users is verified to prevent the creation of an account by an impersonator, to help prevent fraud, including public health care fraud, and to ensure patient safety (as inaccurate patient identification can lead to patient safety issues)", and "Identity verification is critically important for the provision of healthcare delivered in the virtual care context…".

[203] Babylon and the physicians asserted that "The software that is used to verify identity is an automated and far more effective and accurate version of the manual identity verification process that occurs in a doctor's office," and said "This identity verification process has been successfully implemented ubiquitously across multiple sectors, including the financial services sector, to prevent fraud and address other legal obligations. It provides a secure, convenient and effective identify verification process for patients."

[204] Babylon and the physicians concluded their submission by saying, "In sum, the Interested Parties consider this identity verification process crucial to help detect and prevent fraud and ensure patient safety, and, accordingly, cannot discontinue its use".

[205] I considered this submission, but was not persuaded by it. In particular, I note that section 58 (1) of HIA states the following:

> **Duty to collect, use or disclose health information in a limited manner**
>
> 58(1) When collecting, using or disclosing health information, a custodian must, in addition to complying with section 57, collect, use or disclose only the amount of health information that is essential to enable the custodian or the recipient of the information, as the case may be, to carry out the intended purpose.

[206] There is a clear emphasis in section 58 that custodians must limit the collection, use and disclosure of health information to what is **essential** to enable **the custodian** or recipient to carry out the intended purpose. I previously acknowledged that verifying identity is essential for custodians to deliver health care services; however, I reiterate that it is not essential that the physicians (through Babylon) collect copies of government-issued identification and a selfie photograph for this purpose.

[207] I note that guidance provided by other associations and professional bodies support alternatives to collecting copies of identification for the purposes of verifying identity. For example, the Canadian Medical Association, in conjunction with The College of Family Physicians of Canada and Royal College of Physicians and Surgeons of Canada, has published a *Virtual Care Playbook*, which provides the following advice regarding verifying a patient's identity:[15]

> At the beginning of the video connection with the patient, perform the following verifications, disclosures and consent actions (see Appendix A for suggested text):
>
> - Authenticate the patient's identity — if it's a first encounter, ask the patient to hold up a piece of valid government-issued photo ID to the camera to confirm who they are. But, if you already know the patient by sight, that will suffice.

[208] In another example, Doctors of BC has published a *Doctors Technology Office: Virtual Care Toolkit*.[16] This toolkit also suggests that identity verification can be accomplished in ways that do not involve the collection of identification documents or selfie photos. In its enclosed Appendix B, that guidance document states the following regarding validation options:

> Options for Validating:
>
> Option 1: Provide your contact information to the Client and ask them to send the first message;
>
> Option 2: Send an initial text or email (see APPENDIX B) to confirm you have connected with the right individual; or,
>
> Option 3: Ask the recipient to verify, by text or phone, information that only the intended recipient would know (e.g. month/year of birth, last 4 digits of PHN, reference number, date of last clinic visit, or other previously agreed upon information).

[209] Further, Alberta Health Services' (AHS) *Virtual Health Support Kit for Zoom* provides the following guidance for health care providers when registering patients for a Zoom virtual care appointment:[17]

- When requesting patients to register for a Zoom appointment, please limit collection of identifiable health information to their first name, last name, and/or email address. This complies with AHS Zoom privacy requirements.
- Clinicians are to introduce themselves by Name, Occupation and Department (NOD).
- Verify patient identity using approved Patient Identifiers refer to the AHS Patient Identification Policy and the Virtual Health Provider & Patient Identity Verification recommendation.

---

[15] Canadian Medical Association, The College of Family Physicians of Canada and Royal College of Physicians and Surgeons of Canada, "Virtual Care Playbook", March 2020.
[16] Doctors of BC, "Doctors Technology Office: Virtual Care Toolkit", February 23, 2021.
[17] Alberta Health Services, "Virtual Health Support Kit for Zoom", July 10, 2020.

[210] Additionally, AHS's Virtual Health Provider & Patient Identity Verification recommendation states:[18]

> Patient Identity Verification in Virtual Care:
>
> To ensure that the correct patient receives the intended health service, AHS current policy specifies two (2) or more patient identifiers must be used to verify the patient's identity prior to a health service being provided. This applies to virtual visits as well. At the beginning of a virtual care appointment, the health care provider shall verify a patient's identity by:
>
> 1. Asking the patient to verbally state at least two (2) accepted patient identifiers that are listed in the [AHS Patient Identification Policy – PS06].
>
> 2. Matching and verifying the two (2) or more identifiers stated by the patient with the documentation outlining the health service to be provided (e.g., patient chart).

[211] Finally, the Alberta Medical Association published a document entitled *Virtual Care: Helping physicians minimize the risk of exposure to COVID-19*, which includes guidance regarding confirming patient identity when providing virtual care.[19] It states:

> **Confirm patient identity**
>
> If a patient is previously known to the physician or staff, identity verification may be as simple as recognizing each other's voice.
>
> If not, ensure a process is in place to verify identity of the patient or their agent. This can be done by asking for full name, date of birth and one other key piece of information such as postal code

[212] The OIPC has received and accepted numerous PIAs for virtual care applications that do not collect copies of identification or selfie photos. In my view, identity verification can be accomplished in ways that do not involve the collection of this information. Therefore, I find the physicians have collected and used more health information than is essential to carry out intended purposes of verifying an individual's identity to prevent fraudulent use of health services and mismatched patient records.

Finding

- Collecting and using individuals' government-issued identification and selfie photos through the Babylon app goes beyond what is required to provide health services. Therefore, the custodians (physicians) have not met the requirement to collect and use health information in a limited manner as required by section 58 of HIA.

[18] Alberta Health Services, "Virtual Health Recommendation: Provider and Patient Identity Verification in Virtual Care", April 15, 2020.
[19] Alberta Medical Association, "Virtual Care: Helping physicians minimize the risk of exposure to COVID-19", March 11, 2021.

Recommendation

- I recommend that the physicians discontinue the collection and use of government-issued identification and selfie photos.

Recording Consultations

[213] At the time this investigation was launched, patients also had the option within the Babylon app to record the video session of their encounter with a physician. With regard to this collection, the Babylon by TELUS Health Privacy Policy states:

> We retain recordings of our consultations and interactions with you. This can include…video and audio recordings or audio-only recordings…

[214] The "What we use your personal data for" section of the Privacy Policy also says:

> We obtain and use your medical information because this is necessary for medical purposes, including medical diagnosis and the provision of healthcare or treatment. This includes the information collected through our consultations with you (such as notes and recordings), our digital services, and medical history from your previous GP. …

[215] I asked Babylon to provide information regarding its purpose for collecting and recording video interactions between patients and physicians. Babylon responded:

> The recording of interactions between patients and Babylon physicians is an optional feature that is offered to the patient in the event that they want to be able to refer back to the consultation at a later date. Patients do not have to consent to have their interaction recorded as a condition of using the service.

[216] In my view, physicians recording consultations by **taking notes** and entering information into an electronic medical record when providing health services is consistent with typical practices when similar services are provided in-person, and is an essential component of providing health services and meeting professional standards. It may be essential in some cases to obtain a video or audio recording to provide certain medical services in specific circumstances; however, as a general rule, it is not common practice to record audio or video encounters.[20]

[217] It is not clear to me, however, why physicians would retain a video or audio recording of the consultation for general purposes, given the physician is also making notes of the encounter and recording that information in Babylon's electronic medical record. It is not a common practice for physical clinics to record video or audio encounters of patients' in-person visits with their physicians. Furthermore, video and audio recordings collect image, demeanor, voice or other attributes that may not be necessary and are

[20] In these circumstances, written consent must be obtained. See additional requirements for consent under section 23 of HIA.

likely not essential to enabling the custodian to carry out the purpose of providing health services. Therefore, collecting and retaining copies of video interactions of a patient's interaction with their physician is not essential for the custodian physicians to carry out their purposes.

[218] In response to this finding, Babylon and the physicians made an additional submission, saying, in part:

> A recording serves two wholly reasonable and important intended purposes that benefit patients. Specifically (i) recordings are used for quality control purposes, and (ii) recordings enhance the patient record, and can be accessed by the patient upon request. It is clearly necessary and entirely reasonable for these purposes to record the consultation, on an entirely optional basis with the patient's explicit consent. This finding effectively takes choice away from the user.

[219] I considered these assertions; however, for reasons previously given, I maintain my findings and recommendations with regard to the recording of audio and video during virtual consultations. I note again that, while it may be useful for a patient to have copies of recordings, section 58 of HIA limits the collection, use and disclosure of health information to that which is **essential** for the **custodian to carry out the intended purpose**.

[220] I also note that other associations have published guidance cautioning physicians against the use of recordings in a virtual care setting. In one example, The Canadian Medical Protective Association (CMPA) has published an article entitled *Providing virtual care during the COVID-19 pandemic,* which includes the following advice:[21]

> **Privacy and confidentiality**
>
> - Make best efforts to protect patients' privacy in the provision of virtual care. Consider confirming the identity of the person you are interacting with at the beginning of the encounter, **disabling options to record the encounter**, and encouraging people to participate in a private setting. [emphasis added]

[221] In another example, the *Doctors Technology Office: Virtual Care Toolkit*, published by the Doctors of BC, states the following regarding the recording of virtual care appointments:[22]

> - **Avoid recording videoconference sessions** containing personal or clinical information unless it is absolutely necessary. If a recording must be made, the best practice is to retain it as part of the clinical record. Implement security measures such as secure storage behind a firewall. When using personal, mobile and desktop devices, the best practice is to encrypt a device and use two-factor authentication for access. (Please reach out to DTOinfo@doctorsofbc.ca for support on how to do this). [emphasis in original]

[21] Canadian Medical Protective Association, "Providing virtual care during the COVID-19 pandemic", March 2021.
[22] Doctors of BC, "Doctors Technology Office: Virtual Care Toolkit", February 23, 2021.

[222] Overall, I maintain my finding that collecting and retaining copies of video interactions of a patient's interaction with their physician is not essential for the custodian physicians to carry out their purposes.

Finding

- Collecting and using audio and video consultations through the Babylon app goes beyond what is required to provide a health service. Therefore, the custodians (physicians) have not met the requirement to collect and use health information in a limited manner as required by section 58 of HIA.

Recommendation

- I recommend that the physicians discontinue recording of audio and video during virtual consultations with individuals.

Location Data

[223] The "What we use your personal data for" section of Babylon's Privacy Policy describes the collection and use of location data through the app as follows:

> We may obtain and use data about your precise location where you give your consent (through providing us access to your location through your App or browser settings or your address), for example, to help direct you to the nearest pharmacy. We may also derive your approximate location from your IP address.

[224] In my view, collecting precise location in order to direct individuals to the closest pharmacy and "approximate location from your IP address" are not essential to the provision of health services. Directing an individual to a pharmacy, either by the use of an individual's precise location or approximate location obtained from an IP address is not a health service under HIA.

[225] Babylon responded to this finding by saying, in part:

> It is essential to the intended purpose of providing a location-based find a pharmacy feature, to collect a user's location. This feature is entirely optional and location data is collected with express consent. It is wholly unclear why the OIPC would render a decision that precludes users from making an informed choice to avail themselves of such a convenient feature should they find it helpful to do so.

[226] As I have previously stated, section 58 of HIA limits the collection, use and disclosure of health information to what is **essential** for the **custodian** to carry out the intended purpose. Section 20 of HIA must also be considered in understanding the context of section 58 of HIA. Section 20 states the following:

> 20 A custodian may collect individually identifying health information

> (a) if the collection of that information is expressly authorized by an enactment of Alberta or Canada, or
> (b) if that information **relates directly to and is necessary to enable the custodian to carry out a purpose** that is authorized under section 27. [emphasis added]

[227] I am not persuaded that "providing a location-based find a pharmacy feature" is essential for a physician custodian to carry out a purpose authorized under section 27 of HIA. The fact that the feature is "entirely optional" and only with express consent supports my finding.

Finding

- Collecting location data through the Babylon app goes beyond what is required to provide a health service. Therefore, the custodians (physicians) have not met the requirement to collect and use health information in a limited manner as required by section 58 of HIA.

Recommendation

- I recommend that the physicians discontinue the collection and use of precise and approximate location of individuals.

Summary of Findings

[228] My findings from the investigation are:

- The custodians (physicians) have not met the requirement of section 63 of HIA to establish or adopt policies and procedures that will facilitate the implementation of HIA and the regulations.

- The custodians (physicians) did not meet the requirement of section 64 of HIA to prepare and submit a privacy impact assessment prior to adopting the Babylon application to provide health services.

- With respect to services provided under employment/contract with Babylon, the custodians (physicians) have not entered into agreement(s) with an information manager, as required by section 66 of HIA and 7.2 of the *Health Information Regulation*.

- The custodians (physicians) have not met the requirements of section 8(4) of the *Health Information Regulation*, with respect to health information that is stored or used by a person in a jurisdiction outside Alberta.

- The custodians (physicians) have not taken reasonable steps to maintain administrative and technical safeguards to protect health information as required by sections 60 and 63 of HIA, and Section 8 of the *Health Information Regulation*.

- Collecting and using individuals' government-issued identification and selfie photos through the Babylon app goes beyond what is required to provide health services. Therefore, the custodians (physicians) have not met the requirement to collect and use health information in a limited manner as required by section 58 of HIA.

- Collecting and using audio and video consultations through the Babylon app goes beyond what is required to provide a health service. Therefore, the custodians (physicians) have not met the requirement to collect and use health information in a limited manner as required by section 58 of HIA.

- Collecting location data through the Babylon app goes beyond what is required to provide a health service. Therefore, the custodians (physicians) have not met the requirement to collect and use health information in a limited manner as required by section 58 of HIA.

Summary of Recommendations

[229] Based on my findings from and during this investigation, I recommend the physicians:

- Review and update all policies to include relevant approvals and effective date as well as ensure that all privacy policies developed by Babylon and adopted by the physicians clearly outline the responsibilities of the physicians and their affiliates under HIA.

- Prepare and submit a privacy impact assessment that follows the requirements outlined in the *Privacy Impact Assessment Requirements* document, to the OIPC. In addition, all physicians in the future should have to review and sign-off on the PIA as part of their employment terms with Babylon.

- Enter into an information manager agreement with Babylon that meets the requirements of section 66 of HIA and 7.2 of the *Health Information Regulation*.

- Review and revise existing agreements to ensure they meet the requirements of section 8(4) of the *Health Information Regulation*. In addition, the physicians should provide the OIPC with a copy of updated agreements as well as an updated PIA within six months from the date of this report.

- Ensure that any privacy and security awareness training that is provided by Babylon and adopted by the physicians is updated to include references to HIA and its associated requirements.

- Ensure that privacy and security awareness training includes references to the policies that are provided to Alberta-based physicians.

- Develop and implement a proactive auditing process for user access within the Babylon application, to identify and respond to inappropriate access to health information.

- Modify the confidentiality clauses within employment agreements to include relevant references to HIA and to health information. Ensure employees review and sign confidentiality agreements on a regular basis.

- Discontinue the collection and use of government-issued identification and selfie photos.

- Discontinue recording of audio and video during virtual consultations with individuals.

- Discontinue the collection and use of precise and approximate location of individuals.

Closing Comments

[230] This was a complex and multi-faceted investigation that progressed through a number of phases. My findings and analyses are based on the status at the time the initial investigation was launched, April 20, 2020.

[231] During the course of this investigation, Babylon and TELUS engaged with us and started taking steps toward remediating some of the privacy issues that were identified.

[232] As mentioned previously in the report, on January 18, 2021 TELUS acquired the Canadian operations of Babylon Health. In addition, as of June 1, 2021, the Babylon by TELUS Health app was rebranded to TELUS Health MyCare. As part of its acquisition and rebrand activities, TELUS has indicated that as of May 31, 2021, TELUS Health MyCare has made the following enhancements:

> All previous Babylon policies have been replaced with new TELUS Health MyCare policies, which include approvals and effective date. The policies clearly outline the responsibilities of the physicians and their affiliates under the HIA. While the service is supported by the overall TELUS privacy management program and structure, an Alberta-specific Custodian Privacy & Security Policy Manual (to which all relevant policies are appended) has been developed to ensure that all HIA requirements are met. All physicians review and adopt the policies and procedures in the Custodian Privacy & Security Manual when they sign the Information Manager Agreement, which is a schedule to the Independent Contractor Agreement. Any updates to the policies and procedures are documented in the Manual. The Lead Custodian coordinates the review and approval by the physicians of any material changes to the Information Management Policies…
>
> Every Babylon physician endorsed the existing PIA and all Babylon physicians signed PIA Endorsement Letters, which were provided to the OIPC.TELUS is preparing, for submission to the OIPC, updated PIAs that follow the requirements outlined in the Privacy Impact Assessment Requirements document and outline all of the controls, policies and procedures that have been put in place for TELUS Health MyCare. Target submission date is early Fall 2021. All physicians will be required to review and endorse the updated PIAs. Moving forward, any net new PIAs will be reviewed and endorsed by each custodian. The review of any updates to existing PIAs will be coordinated by the Lead Custodian, who will sign off on the updates on behalf of the Custodians...
>
> Babylon Canada and the physicians entered into an Information Manager Agreement ("IMA") that outlines the custodian relationship and meets the requirements of s. 66 of the HIA and 7.2 of the Health Information Regulation. The IMAs between the physicians and Babylon have been adopted by TELUS. All physicians have entered or are currently entering into a new IMA with TELUS, the terms of which meet the requirements of s. 66 of the HIA and s. 7.2 of the Health Information Regulation. Physicians' responses to the IMA were sent to the OIPC between September 4, 2020 and October 19, 2020…
>
> Babylon Canada and the physicians entered into an IMA, the terms of which met the requirements of s. 8(4) of the Health Information Regulation. All physicians have entered or are currently entering into a new IMA with TELUS, the terms of which meet the requirements of s. 8(4) of the Health Information Regulation. TELUS is preparing, for submission to the OIPC, updated PIAs that follow the requirements outlined in the Privacy Impact Assessment Requirements document and outline all of the controls, policies and procedures that have been put in place for TELUS Health MyCare, including with respect to the use of third party service providers operating in jurisdictions outside Alberta.

> Target submission date is early Fall 2021. Once per calendar year, TELUS will attest in writing to the Lead Custodian that it continues to meet its obligations under the IMA as it relates to third-party services that may impact Health Information…
>
> [T]he physicians have all completed updated training that includes references to the HIA and its associated requirements. TELUS Health MyCare privacy and security awareness training has been developed and also meets this requirement…
>
> TELUS' Compliance Monitoring Program measures business units including clinics, on a regular basis against a set of key compliance indicators established by the Data & Trust Office. Summary reports of the results are prepared for the appropriate executive and the Lead Custodian to enable a clear line of sight into the efficacy of existing policies, standards and procedures and include suggested remediation actions to address any gaps. TELUS has a formal audit program. The Audit team conducts privacy and security audits from time to time, as part of their rotating audit schedule, including audits of compliance with privacy policies. Opportunities for improvement in a clinic are identified and assigned to the Lead Custodian for remediation within a specified timeframe. TELUS has implemented the application of logging requirements, which are documented in a policy appended to the Alberta Custodian Privacy & Security Manual. Clinics are required to ensure that proactive monitoring of access logs and oversight tools for inappropriate access is in place…
>
> In relation to its acquisition and rebranding activities, TELUS is implementing a new confidentiality agreement that specifically addresses the HIA. Employees will be required to sign the confidentiality agreement upon hire and on an annual basis…
>
> Video recording functionality was turned off in June of 2020. The 'toggle' to consent to audio"…
>
> [C]onsultations within the app is now set to 'off' and, as was the case at the start of the investigation, express consent is also collected verbally during the consultation with a healthcare practitioner. This results in what is, in fact, a double express consent before a consultation is recorded."

[233] I would like to thank Babylon and TELUS for their cooperation and transparency through the investigation process, and their efforts to date to comply with recommendations made in this report. I request that TELUS report back within 6 months on its progress complying with the remaining outstanding recommendations.

[234] As we move toward an increasingly interconnected and technologically advanced world, with increased popularity and availability of virtual care platforms, it is important for custodians to remain aware of their obligations under HIA. Custodians must be vigilant in ensuring that, when they adopt a virtual care platform, not only do they comply with the requirements set out in HIA, they ensure their service providers also comply with HIA. This includes proactively taking steps to review the requirements of privacy legislation for new jurisdictions in which they would like to expand their services.

Christine Sereda
Senior Information and Privacy Manager