Office of the Information and
Privacy Commissioner of Alberta

# Investigation Report P2021-IR-02

***Investigation into Babylon by TELUS Health's compliance with Alberta's* Personal Information Protection Act**

**July 29, 2021**

*Babylon Health Canada Ltd.*

*Investigation 015681*

# 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). The PIPA investigation focused on the app's non-medical digital healthcare tools (Symptom Checker and Healthcheck), as well as virtual consultations with dietitians and mental health counsellors.[1]

Key findings from the investigation are:

- Overall, Babylon collects, uses and discloses personal information for reasonable purposes and to a reasonable extent. This includes personal information collected, used and disclosed as part of consultations with dietitians and mental health counselors, audio and video recordings, financial information to obtain payment for billable services, and basic contact information for marketing and communications purposes.

- In some cases, Babylon collects more information than is reasonable for some purposes. Of particular concern is the collection and use of copies of government-issued identification and a selfie photograph that are "checked, matched and verified through use of technology", before an appointment is booked with a dietitian or mental health counsellor. Babylon did not establish that it is reasonable to collect this extent of personal information in order to verify identity, and detect and prevent fraud.

- Babylon's Privacy Policy did not clearly identify the purposes for which personal information is collected, nor what information is associated with each purpose. The investigation found that it was unlikely individuals would review the lengthy linked documents on mobile devices before personal information is collected. Another issue was that the Privacy Policy included information on functionality that was not enabled or available to individuals.

- Babylon engages services providers outside of Canada, including Ireland, Europe, the Middle East, Africa, the UK and the USA. However, Babylon did not meet the requirements in PIPA

[1] Dietitians and mental health counselors are not custodians providing health services, such that their activities would be subject to Alberta's *Health Information Act*. Instead, PIPA applies.

to develop policies and practices that include information regarding the countries in which personal information is collected, used, disclosed or stored, and the purposes for which service providers outside of Canada are authorized to collect, use or disclose personal information. Babylon did not meet the requirement to notify individuals about how they can obtain information about the collection, use, disclosure or storage of personal information by service providers outside of Canada.

With respect to Babylon's consent practices, the investigation found:

- Babylon cannot rely on the combination of its privacy policy and the consent toggle for express consent because the privacy policy is linked, lengthy, unclear and contains inaccuracies.
- Deemed consent may be appropriate in some circumstances; however, there are examples in the app where the purposes for collection may not be obvious, and it may not be reasonable that a user would voluntarily provide information.
- Where Babylon wishes to rely on opt-out consent, it must provide an easy to understand notice and a clear opportunity to opt-out. This option will not usually be appropriate when sensitive information is at issue.

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 some of the compliance issues identified through the investigation, primarily with regard to implementing a new Privacy Commitment and FAQ.

We have requested that Babylon report back within six months on progress complying with the remaining outstanding recommendations.

As a consequence of the pandemic, we are seeing widespread and accelerated development and implementation of virtual healthcare technologies. These technologies can be innovative, effective and popular. However, they can also be complicated and sophisticated, and often involve myriad, complex information flows and transactions behind the scenes. Alberta's PIPA requires organizations to limit their collection of information to what is reasonable to meet reasonable purposes, and to be transparent and clear about what personal information is collected for what purposes, and where that information may be accessed or stored. Complying with these legal requirements helps to ensure that individuals are able to make informed decisions about whether and to what extent they wish to engage with new technologies.

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 Custodian 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[2]:

> 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.[3,4]

[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

[2] Government of Alberta, "New app helps Albertans access health care", March 19, 2020.
[3] Alberta Medical Association, "Babylon: setting the record straight", March 21, 2020.
[4] 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 PIPA investigation said:

> Several factors led me to opening this investigation under PIPA. 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] I was assigned to conduct the investigation.

[13] 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."

[14] Notwithstanding this, my investigation is concerned with the operation and implementation of the app at the time this investigation was initiated on April 20, 2020.

[15] This report sets out the findings and recommendations from my investigation.

# Background

[16] The Babylon by TELUS Health app is described in Babylon's Terms and Conditions document, as provided by Babylon, which says that Babylon's "Services" include "(i) symptom checker; (ii) Healthcheck and (iii) Monitor tools". The monitor function was not available at the time this investigation was initiated and was not reviewed as part of this investigation. The Symptom Checker and Healthcheck tools were available, however, and are described in the Terms and Conditions as follows:

> - Our **symptom checker** will provide different types of information to you based on, amongst other things, the symptoms entered. One possible output of the symptom checker is the more detailed next steps someone experiencing the symptoms entered would usually take ("Triage"). The other possible output is general medical information on the types of conditions that people who have experienced similar symptoms have had, which may include less detailed typical next steps...
>
> - For our **Healthcheck** tool:
>
>  - Healthcheck is an information and educational tool to help you understand risk rates for certain conditions based on the information entered. It may provide information on factors which are known generally to help achieve a healthy lifestyle.
>  - By completing and submitting the Healthcheck questionnaire, our software provides a report based on general statistical information of certain diseases and conditions ...
>  - Reports are produced on the basis of information you enter only and are based on general statistical information and risk factors only. Reports are responsive to information entered, but are not personalised to you. We will not be able to provide information on risk factors which are not entered... [emphasis in original]

[17] The Terms and Conditions are clear that these digital healthcare tools...

> ...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[5]]

[18] In addition to the above, however, Babylon does provide "health and medical advice", and "diagnosis and/or treatment" through the app in some provinces, including Alberta. The Terms and Conditions defines these "Clinical Services" as follows:

> - In some provinces, we provide health and medical advice via our video and audio doctor consultations (not available in all provinces or territories). Today, this feature is currently only available in British Columbia, Alberta, Ontario, Quebec and Saskatchewan.
>
> - Except where we provide clinical services via our video and audio consultations with our Practitioners ("Clinical Services"), the Services, including our digital healthcare tools, (i.e. our

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

> Symptom Checker, Healthcheck and Monitor) within the App do not provide medical advice, diagnosis and/or treatment and do not form part of the Clinical Services. Except for Clinical Services, the output from the Services also does not constitute medical advice, diagnosis or treatment… [emphasis removed from original]

[19] The Terms and Conditions also say "Clinical Services" 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] Clinical Services are delivered by "Practitioners", including "Medical Professionals" and "Allied Professionals", which are 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" or "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.

# 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 organization in digital health that combines the benefits of [Artificial Intelligence] with the medical expertise of doctors".[6] 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. Babylon UK describes Babylon's role as follows:

- Babylon is the service provider of the Babylon by TELUS Health App services;
- Babylon distributes the Babylon by TELUS Health App to individual end users in Canada;
- End users contract with Babylon for the Babylon by TELUS Health App services;
- Babylon provides clinical and AI 'symptom checker' services to end users of the Babylon by TELUS Health App; and
- Babylon controls, runs and manages the Babylon by TELUS Health App and the global Babylon App.

[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.

***Personal Information Protection Act (PIPA)***

[26] Alberta's PIPA applies to "organizations" with respect to the collection, use and disclosure of "personal information" in Alberta.

[27] Section 1(1)(i)(i) of PIPA defines an "organization" to include "a corporation". Babylon UK and Babylon are both "organizations" as defined in section 1(1)(i)(i).

[28] Individual users download the Babylon by TELUS Health app to their mobile device by completing a registration process and creating login credentials. Through the registration process, identifiers such as first and last name, email address, and physical address including postal code are collected. Once registered and in the application, the individual is able to interact with the Symptom Checker or Healthcheck functions by entering symptoms or completing and submitting the Healthcheck questionnaire.

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

[29] Individuals are also able to access Clinical Services through the app. To access these services, individuals must book an appointment, which requires the individual to verify their identity by submitting a selfie photograph and a photo of identification, such as a driver's licence, passport, national identity card or permanent residence card. Individuals will then participate in remote video and voice consultations with Babylon's Practitioners.

[30] All of the above is information about identifiable individuals and qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

***Health Information Act (HIA)***

[31] Section 4(3)(f) of PIPA says that the Act "does not apply to the following:... (f) health information as defined in the *Health Information Act* to which that Act applies."

[32] Alberta's *Health Information Act* (HIA) applies to "health information" that is collected, used or disclosed by a "custodian".

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

[34] "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,

[35] "Diagnostic, treatment and care information" is defined in section 1(1)(i) and includes:

> (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

[36] "Health service" is defined in section 1(1)(m) as follows:

> (m) health service" means a service that is provided to an individual for any of the following purposes:
>
> (i) protecting, promoting or maintaining physical and mental health;
> (ii) preventing illness;
> (iii) diagnosing and treating illness;
> (iv) rehabilitation;

(v) caring for the health needs of the ill, disabled, injured or dying,

but does not include a service excluded by the regulations

[37] The "general health information" returned to users through Babylon's digital healthcare tools (i.e. Symptom Checker and Healthcheck) is generated by artificial intelligence (AI), and "no Practitioner is involved in providing the information". There is no custodian involved, and no "health service" as defined in HIA.

[38] As a result, any information about users that is collected, used and disclosed by Babylon in the course of providing these digital services is subject to PIPA. This information is personal information about identifiable individuals to which PIPA applies.

[39] Babylon's Clinical Services, however, include consultations with "Practitioners" (physicians, dietitians and mental health counsellors) who are employed by or contracted to Babylon.

[40] Section 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* designates regulated members of the College of Physicians and Surgeons of Alberta (CPSA) as custodians. Physicians are regulated members of the CPSA and are custodians to which HIA applies.

[41] Consultations with physicians involve the collection, use and potentially disclosure of registration information and diagnostic, treatment and care information, which is "health information" as defined in sections 1(1)(i) and 1(1)(u) of HIA. Therefore, HIA applies to the collection, use and disclosure of this health information by custodians (physicians), in the course of providing health services. Consequently, HIA applies to this information and, pursuant to section 4(3)(f) of PIPA, PIPA does not.

[42] Dietitians and mental health counsellors, however, are **not** custodians as defined in HIA, and HIA does **not** apply to them or any service they offer. Identifiable information collected, used or disclosed by these Practitioners is not "health information as defined in the *Health Information Act* to which that Act applies" such that it would be excluded from the application of PIPA by virtue of section 4(3)(f). Instead, this information is about identifiable individuals and is personal information as defined in PIPA. Therefore, PIPA applies to the collection, use and disclosure of personal information by dietitians and mental health counsellors in the course of providing Clinical Services.

***Dietitians and Mental Health Counsellors***

[43] As noted above, dietitians and mental health counsellors are not custodians as defined in HIA, and PIPA applies the collection, use and disclosure of personal information by dietitians and mental health counsellors.

[44] Section 5(2) of PIPA reads:

> (2) For the purposes of this Act, where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with this Act.

[45] Babylon employs or contracts dietitians and mental health counsellors, and therefore "engages the services" of dietitians and mental health counsellors and is responsible for their compliance with PIPA.

[46] For dietitians and mental health counsellors who are contracted to Babylon, section 5(6) of PIPA reads:

> (6) Nothing in subsection (2) is to be construed so as to relieve any person from that person's responsibilities or obligations under this Act.

***TELUS Health Solutions Inc.***

[47] TELUS Health Solutions Inc. (TELUS Health) is a division of TELUS Corporation and is described by Babylon UK as follows:

> TELUS Health leverages technology to enable better health outcomes for Canadians with innovative digital solutions that enable collaboration, efficiency and productivity for physicians, pharmacists, health authorities, allied healthcare professionals, insurers, employers and citizens.

[48] TELUS Health operates across Canada, including in Alberta, and is an "organization" as defined in section 1(1)(i) of PIPA.

[49] Babylon UK describes the role of TELUS Health in the delivery of the Babylon by TELUS Health app as follows:

- TELUS provides branding, marketing and sales channels for the Babylon by TELUS Health App in Canada;
- TELUS provides requirements and funding to develop and localize the Canadian version of the app;
- TELUS resells the Babylon by TELUS Health App to Enterprise Customers and Government Customers in Canada; and
- TELUS provides the cloud hosting environment for the Babylon by TELUS Health App. TELUS provides 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 by TELUS Health App.

[50] Babylon UK also explained that, "TELUS and Babylon Health Canada ("Babylon") have entered into a commercial relationship (on the terms set out within their contractual agreement) to deliver Babylon's technology services to Canada". Babylon UK provided excerpts from this "Contractual Agreement", including portions of the following:

- "Section 5: Managed Services"
- "Section 13: Localization Requirements"

- "Section 14.6: Privacy and Security"
- "Schedule D: Telus Health Cloud Service Access Terms and Security Requirements"
- "Clause 1.2: Use of TELUS Health Cloud Platform"
- "Clause 1.5: Security Breach Notifications"
- "Schedule J: Privacy Requirements"
- "Clause 14.7: Ownership and Use of Data"
- "Section 14.8: Representations Related to De-Identified Data"
- "Clause 14.9: De-identified Data and Personal Information"

[51] From my review of these materials, I understand that Babylon provides the Babylon by TELUS Health app and services, and, by virtue of a contract between Babylon and TELUS Health, TELUS Health provides services to support the "making available all services provided to and through the Babylon by TELUS Health App", including branding, marketing and sales, and access to the TELUS Health cloud hosting environment.

[52] As such, section 5 of PIPA is relevant:

> 5(1) An organization is responsible for personal information that is in its custody or under its control.
>
> (2) For the purposes of this Act, where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with this Act
>
> …
>
> (6) Nothing in subsection (2) is to be construed so as to relieve any person from that person's responsibilities or obligations under this Act.

[53] In my view, Babylon has engaged the services of a person (TELUS Health) and is, with respect to those services, responsible for TELUS Health's compliance with PIPA, as contemplated by section 5(2) of PIPA.

***Other Third-Party Service Providers***

[54] As previously described, Babylon UK is the parent company to Babylon, and established the latter to provide the Babylon by TELUS Health app to Canadians.

[55] With respect to the relationship between Babylon UK and Babylon in the provision of these services, 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.

> De-identified usage data may also be accessible in order to provide aggregated reporting to Telus (e.g. number of downloads, number of appointments booked). Subject to users' explicit consent, de-identified data can be used for research and analytics purposes to improve Babylon's products and services.

[56] At the start of this investigation, there was no agreement between Babylon UK and Babylon that included PIPA-related provisions. However, given that Babylon "shares data" with Babylon UK "for the purposes of [the latter] delivering services and providing technical support and maintenance" to Babylon, in my view, Babylon has engaged the services of a person (Babylon UK) "by contract or otherwise" and is, with respect to those services, responsible for Babylon UK's compliance with PIPA, as contemplated by section 5(2) of PIPA.

[57] Babylon UK in turn 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 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.

[58] 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

[59] Section 1(1)(m.3) of PIPA defines service provider as follows:

> "service provider" means any organization, including, without limitation, a parent corporation, subsidiary, affiliate, contractor or subcontractor, that, directly or indirectly, provides a service for or on behalf of another organization;

[60] Pursuant to section 5(2) of PIPA, Babylon is responsible for its service providers' compliance with PIPA when those companies provide services on behalf of Babylon that involve the collection, use or disclosure of personal information. These business relationships require both Babylon and its service providers to comply with PIPA.

## Issues

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

- Issue 1: For what purposes does Babylon collect, use and disclose personal information?

- Issue 2: Does Babylon collect, use and disclose personal information for reasonable purposes and only to the extent that is reasonable for meeting those purposes, as required by sections 11, 16 and 19 of PIPA?

- Issue 3: Does Babylon notify individuals of the purpose(s) for which personal information is collected, as required by section 13 of PIPA?

- Issue 4: Does Babylon use service providers outside Canada to collect, use, disclose or store personal information for or on its behalf? If so, has Babylon met the requirements of sections 6 and 13.1 of PIPA with respect to developing policies and practices and notifying individuals?

- Issue 5: Does Babylon collect, use and disclose personal information with consent (unless otherwise authorized), as required by section 7 of PIPA?

## Methodology

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

- Met and communicated in writing with representatives of Babylon, Babylon UK, TELUS Corporation and TELUS Health
- Sent written questions to and reviewed responses provided by Babylon and Babylon UK
- Requested and reviewed copies of documentation, including policies, procedures, data flows, contract excerpts and risk assessments provided by Babylon UK
- Reviewed the two privacy impact assessments (PIA) submitted by Dr. Keir Peterson, and the PIA submitted by Dr. Renie Traiforos
- Downloaded the Babylon by TELUS Health app
- Sent a draft investigation report to Babylon for fact checking, considered Babylon's feedback and finalized the report

# Analysis, Findings and Recommendations

## Issue 1: For what purposes does Babylon collect, use and disclose personal information?

[63] Before considering Babylon's compliance with PIPA, I found it necessary to identify the purposes for which Babylon collects, uses and discloses personal information. These purposes are described in Babylon's Privacy Policy (Appendix A), and sections 3 and 4 in particular. I reviewed the Privacy Policy, and have noted relevant excerpts below under the headings and subheadings that appear in the Privacy Policy.[7]

***Section 3- "What we use your personal data for"***

*"Providing you a service"*

[64] This section of the Privacy Policy describes various purposes for collecting, using and disclosing personal information, including "in order to establish and deliver our contract with you and (if applicable) charge you correctly".

[65] This section also describes collecting, using and retaining "medical information because this is necessary for medical purposes, including medical diagnosis and the provision of healthcare or treatment", as well as "sharing information with other healthcare professionals as necessary for the provision of care to you". The Privacy Policy says that Babylon's physicians and their designates may access medical and/or prescription history "contained within provincial databases (including but not limited to, PharmaNet, NetCare, Drug Profile Viewer) for the purpose of providing care or for the purpose of monitoring medication use".

*"Making healthcare accessible"*

[66] This section of the Privacy Policy describes using "medical information (always having removed personal identifiers, such as your name, address and contact details) to improve our healthcare products and services, and our artificial intelligence system, so that we can deliver better healthcare to you and other Babylon users".

[67] The Privacy Policy notes that use of this data is "only about improving our products, services and software so that we can deliver a better experience to you and other Babylon users, and help achieve our aim of making healthcare affordable and accessible to everyone".

[7] The Privacy Policy referenced in this report is the version that was in place at the start of this investigation. The Privacy Policy was revised during the course of the investigation; however, the observations and analysis here still apply.

[68] This section also says that Babylon "may obtain and use data about your precise location... to help direct you to the nearest pharmacy".

*"Keeping you up to date"*

[69] This section of the Privacy Policy includes such purposes as contacting users to provide appointment reminders, offer "helpful information", and to invite users to make appointments. This section also describes contacting users or presenting them with updates and marketing messages.

*"Other uses"*

[70] This section of the Privacy Policy describes a number of "Other uses" for which Babylon collects, uses and discloses personal information, including:

- To "troubleshoot bugs within the App or our website, forecast demand of service and to understand other trends in use, including which features users use the most and find most helpful, and what features users require from us". Specifically, this purpose is about "improving our App so that we can deliver better services to you"

- Sharing "personal and financial details for the purposes of fraud prevention and detection".

- Storing "medical information, such as notes from consultations, recordings of our consultations with you as well as your interactions with our digital services... for safety, regulatory, and compliance purposes". The Privacy Policy notes that information may be disclosed where necessary "in compliance with lawful requests by regulatory bodies or as otherwise required by law or regulation".

- Auditing consultations and "other interactions with our services" where "necessary for safety, regulatory and/or compliance purposes".

***Section 4 – "Sharing your personal data with others"***

[71] This section of the Privacy Policy describes the purposes for which personal information is shared with various third parties, including:

- The Privacy Policy notes that Babylon has "partnered with TELUS Health to provide certain services on our behalf, including technical and customer support and communications" and that "personal data will be shared with TELUS Health as necessary to allow TELUS Health to provide these services to you and to us." This section says that, "With your consent… (Babylon) will also share your personal data, such as name and contact details... with TELUS Health so that TELUS Health can tell you about their products or services that might be of interest to you".

- Personal information may be shared "with members of our corporate group to help us deliver our services to you."

- Personal information (with identifiers removed) is shared with members of Babylon's "corporate group to help us develop, improve and maintain our software and artificial intelligence system (where you have optionally explicitly consented to this use of your information)".

- Personal information may be shared with companies Babylon has "hired to provide services on our behalf, such as data hosting and processing, technical support, billing and payment processing, marketing and communications."

- In certain circumstances, and "with consent", Babylon will "let your insurance company know your name, email address, policy number, location (based on IP address), demographic information, that you had an appointment with us, the date of the appointment, details of your diagnosis, prescription, pharmacy location, whether or not you had a referral made and other similar information about your appointment with us".

[72] A portion of this section is titled, "Information sharing with other healthcare providers" and notes that Babylon will "where necessary for your treatment or care, share your information with your other health and social care providers" and this "may include sharing information with such services for safeguarding purposes in accordance with our legal or professional obligations". The same section also says:

> We may preserve or disclose information about you to comply with a law, regulation, legal process, or governmental request; to assert legal rights or defend against legal claims; or to prevent, detect, or investigate illegal activity, fraud, abuse, violations of our terms, or threats to the security of our services or the physical safety of any person.

[73] Overall, from my review of the Privacy Policy, I found it difficult to discern the purposes for which Babylon collects, uses and discloses personal information.

[74] The subheadings are not particularly helpful. For example, most users would likely not understand "Making healthcare accessible" to mean that Babylon collects, uses and discloses personal information to improve Babylon's healthcare products and services, and AI system. This section also describes Babylon's collection of location data in order to direct users to the nearest pharmacy, which is not clearly suggested by the subheading. In another example, the subheading "Other uses" does not suggest to the user that personal information is collected, used and potentially disclosed for troubleshooting the app, fraud prevention and detection, and safety, regulatory and compliance purposes.

[75] Many purposes for which Babylon collects and uses personal information are identified only in Section 4 of the Privacy Policy, which is titled, "Sharing your personal data with others". For example, this section describes providing technical and customer support to

users, as well as communications, data hosting and processing, and billing and payment. These are, in fact, Babylon's own purposes for collecting, using and (in some cases) disclosing personal information.

[76] Nonetheless, from my review, I was able to discern and understand that Babylon collects, uses and discloses personal information for the following eight general purposes:

- Sign-up / registration
- Providing non-medical digital healthcare services (including Symptom Checker and Healthcheck)
- Providing Clinical Services (including medical diagnosis, healthcare and treatment, and prescribing and monitoring medication)
- Billing and payment
- Technical services support (including hosting, troubleshooting, and managing and processing data)
- Legal and regulatory compliance (including fraud detection and prevention)
- Quality improvement (including analytics to improve products, services, software; and "develop, improve and maintain ... software and artificial intelligence system")
- Marketing and communications (including sending updates and marketing communications)

**Finding**

- I find that Babylon collects, uses and discloses personal information for eight general purposes:
    - Sign-up / registration
    - Providing non-medical digital healthcare services (including Symptom Checker and Healthcheck)
    - Providing Clinical Services (including medical diagnosis, healthcare and treatment, and prescribing and monitoring medication)
    - Billing and payment
    - Technical services support (including hosting, troubleshooting, and managing and processing data)
    - Legal and regulatory compliance (including fraud detection and prevention)
    - Quality improvement (including analytics to improve products, services, software; and "develop, improve and maintain ... software and artificial intelligence system")
    - Marketing and communications (including sending updates and marketing communications)

## Issue 2: Does Babylon collect, use and disclose personal information for reasonable purposes and only to the extent that is reasonable for meeting those purposes, as required by sections 11, 16 and 19 of PIPA?

[77] Section 11 of PIPA requires an organization to collect personal information only for purposes that are reasonable, and only to the extent that is reasonable for meeting those purposes. Section 11 says:

> 11(1) An organization may collect personal information only for purposes that are reasonable.
>
> (2) Where an organization collects personal information, it may do so only to the extent that is reasonable for meeting the purposes for which the information is collected.

[78] Sections 16 and 19 read the same, but with respect to use and disclosure of personal information.

[79] Section 2 of PIPA says:

> 2 Where in this Act anything or any matter
>
> (a) is described, characterized or referred to as reasonable or unreasonable, or
> (b) is required or directed to be carried out or otherwise dealt with reasonably or in a reasonable manner,
>
> the standard to be applied under this Act in determining whether the thing or matter is reasonable or unreasonable, or has been carried out or otherwise dealt with reasonably or in a reasonable manner, is what a reasonable person would consider appropriate in the circumstances.

[80] Babylon's Privacy Policy describes the personal information that Babylon collects, uses and discloses. I reviewed this information *vis à vis* the eight general purposes for collection, use and disclosure identified in the previous issue.

***Sign-up / Registration***

[81] When an individual first registers for the app, a "Sign up" page appears, and users are required to provide:

- First and last name
- Email address
- Street address
- Postal code

[82] They must also create a password.

[83] The "What personal data we hold and how we get it" section of Babylon's Privacy Policy refers to this sign-up process and says, "When you register with us, you complete forms

and provide us with basic information about yourself, such as your name, date of birth, physical address and email address".[8]

[84] It is not clear from either the sign-up page or Babylon's Privacy Policy what the purpose is for which users are required to identify themselves, provide contact information, and generate an account user ID at the time they download the app, particularly if they intend only to use the app's free services, such as the Symptom Checker and Healthcheck functions. I note that a variety of websites and apps provide similar functions/services for free and without requiring identifiable information (for example, a Google search or Alberta Health's symptom checker webpage).[9]

[85] In response to this concern, Babylon provided additional information:

> The Babylon by TELUS Health app is meant to be a holistic digital health offering. It is not meant to be an anonymous service. Users are required to create an account in order to access the app's services, which includes clinical services as well as various "selfservice" features, such as the Symptom Checker and Healthcheck service. A key benefit of these self-service tools is that they allow users to maintain records of their interactions. The Symptom Checker and Healthcheck features simply cannot be meaningfully compared to a "Google Search" or Alberta Health's Symptom checker page. Babylon requires users to provide their basic contact information to set up an account to allow for this more holistic and personalized offering. As part of the registration process, Babylon requires only the name, email address and physical address of the user. For clarity, consumer users are not prompted (or otherwise required) to provide their date of birth upon registration for the app. This non-sensitive basic contact information is required to provide the various health services offered through the app and requiring the user to provide this information is otherwise wholly reasonable in connection with the establishment of a secure account and contractual relationship with an individual. We note that requiring this type of basic contact information is a ubiquitous and well-established practice for apps in a broad array of contexts. Moreover, the basic contact information is also used for user safety purposes, as Babylon needs to be able to contact users who are demonstrating concerning activity on the Symptom Checker (e.g., suicidal tendencies or signs of being victims of domestic violence); or who have been given an AI outcome that does not appear to be clinically safe (for example, a recommendation to take pain killers for chest pain when they should be advised to go to the hospital).

[86] In this submission, Babylon says its purpose for requiring individuals to identify themselves is for the "establishment of a secure account and contractual relationship with an individual", to "allow users to maintain records of their interactions", and to "allow for this more holistic and personalized offering". Given this, I accept that Babylon has a reasonable purpose for collecting some personal information, and specifically name and email address, as these are the basic data elements to identify an individual user and set up an account. I note again, however, that these purposes are not made clear when a user registers for the app or from a review of Babylon's Privacy Policy.

---

[8] Despite this statement in the Privacy Policy, users are not prompted to provide date of birth when they sign-up for the app. This inaccuracy is addressed later in this report.

[9] Alberta Health's "MyHealth.Alberta.ca: Check Your Symptoms" webpage.

[87] Babylon did not provide any information to explain why an individual's physical address and postal code are reasonable for this purpose. As a result, I find that the collection of physical address and postal code is beyond what is reasonable to meet Babylon's purpose.

[88] I note also that Babylon's submission says:

> [T]he basic contact information is also used for user safety purposes, as Babylon needs to be able to contact users who are demonstrating concerning activity on the Symptom Checker (e.g., suicidal tendencies or signs of being victims of domestic violence); or who have been given an AI outcome that does not appear to be clinically safe (for example, a recommendation to take pain killers for chest pain when they should be advised to go to the hospital).

[89] I am not persuaded that this is a reasonable purpose for collecting this information. In a separate submission, Babylon said the following with respect to the Symptom Checker:

> The Symptom Checker is powered by AI and is not a real clinician, and the output from the Symptom Checker does not constitute medical advice, diagnosis or treatment; it provides triage advice based on the combination of symptoms that a user enters. We use in-app disclaimers to explain that this product should not be used as a medical diagnosis tool and that it should not be used in an emergency.

[90] Nothing in the above statement indicates that the information that users input into the Symptom Checker is monitored in real time or by employees of Babylon. On the contrary, the statements suggest that the Symptom Checker interactions are limited to AI functionality and that the "product should not be used as a medical diagnosis tool and that it should not be used in an emergency". Babylon has not provided any information to explain how personal information entered at the sign-up page would be used to respond to or follow-up with an individual demonstrating suicidal tendencies, appearing to be a victim of domestic violence, etc. Given this, I am not persuaded that it is reasonable for Babylon to collect this contact information from every individual who registers for the app in order to "contact users who are demonstrating concerning activity on the Symptom Checker". This purpose is not what a reasonable person would consider appropriate in the circumstances. Moreover, this purpose is not made clear at the time users register for the app or in Babylon's Privacy Policy.

**Findings**

- I find Babylon has a reasonable purpose for collecting and using name and email address when an individual signs-up/registers for the app.
- Babylon has not demonstrated that it is reasonable to collect personal information at the registration stage for user safety purposes.
- The collection of physical address and postal code goes beyond what is reasonable for Babylon's stated purposes. Therefore, Babylon has not met the requirements of

sections 11 and 16 of PIPA to collect personal information only to the extent that is reasonable for meeting its purposes.

**Recommendation**

- I recommend that Babylon modify its registration process to eliminate the requirement for individuals to provide physical address and postal code at the time an individual registers for the app.

***Providing Non-Medical Digital Healthcare Services***

[91] During the course of an individual's interactions within the Symptom Checker and Healthcheck tools, the app's AI system asks a number of questions, prompting individuals to provide information. The questions are presented in a series, with each subsequent question being presented as a result of the information provided in response to previous questions. At the very start of the process using the Symptom Checker, individuals are prompted to provide gender and date of birth (it appears Healthcheck users can provide "age" instead of date of birth).

[92] With respect to personal information collected as part of these non-medical digital healthcare services, Babylon's Privacy Policy says:

> The main type of information we hold about you **is health and medical information**: information about your health, symptoms, treatments, test results, consultations and sessions, medications and procedures. **This includes** … **interactions with our digital services, including interactions with our chatbot, symptom checker, 'Ask a doctor', Healthcheck, Digital Twin services, health monitoring, or other health and condition management services**. [emphasis added][10]

[93] The "What we use your personal data for" section of the Privacy Policy 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 digital services**… [emphasis added]

[94] With respect to gender and date of birth specifically, I asked Babylon to explain its purpose for collection. Babylon responded by saying, in part:

> We gather age simply to understand whether it is appropriate to allow access to our services. If the age is >16, we do not allow access under the parent account. We collect gender to appropriately provide medical advice. Afterwards it is stored so that the user can access it after the conversation has ended.

[10] Babylon uses the term "health and medical information", which includes personal information collected by the app's digital services from its users. For the purposes of this report, this information is deemed to be "personal information" under PIPA and not "health information" under HIA.

[95] In a separate response, Babylon said:[11]

> We collect [date of birth] and gender because the clinical outcomes are linked to these variables. For example, if we didn't collect gender we would risk telling male users about female health issues and vice versa. Collection of these data elements provides a more accurate assessment of the conditions being described in the symptom checker.

[96] In my view, it is reasonable for Babylon to collect "health and medical information", in the form of responses to questions posed to users, in order to provide its Symptom Checker and Healthcheck services. These services are intended to return AI-generated "general health information" based on information that the user provides. If an individual wants to use the tools to obtain general health information relevant to them, then the user will need to provide some information for this purpose.

[97] I am concerned, however, that the Symptom Checker function collects date of birth, in association with identifying name and contact information. Babylon advised that it collects "age simply to understand whether it is appropriate to allow access to our services. If the age is >16, we do not allow access under the parent account". While it may be helpful to collect full date of birth to determine if the user is over the age of 16, it seems to me this same purpose could be accomplished by collecting age only (as the Healthcheck function appears to do). For example, the app could ask an individual if they are 16 or over; if the individual responded yes, they could be advised that they need to create their own account and are prevented from going further with the app (which is what the app does currently when full date of birth is provided).

[98] Babylon also said that it collects full date of birth and gender to provide a "more accurate assessment of the conditions being described". Again, I accept that it is reasonable to collect information about age and gender, such that the general, non-medical health information generated by the app's AI will be useful and relevant to the user; however, it is not clear to me why the app would need to collect full date of birth (rather than age).

[99] In response to my concern about the collection and use of full date of birth, Babylon said in a separate submission:

> [C]ollection of date of birth is wholly reasonable and important for patient safety. Collection of date of birth (rather than age) can be important for the accuracy of the output from the Symptom Checker, particularly if a user may be nearing (or recently past) their birthdate. For example, many national recommendations for screening tests — for colon cancer or breast cancer for example — use precise age cut-offs. Not knowing an exact age would therefore mean that the Symptom Checker may inappropriately recommend a screening test before or after it would have ideally been done. Similarly, some medications are not recommended outside of a specific age range. Being off by 11 months could lead to a recommendation to speak with a doctor about a specific medication that they are not eligible for.

[11] Babylon's response also indicated that it collects date of birth "in the event of an issue" and to meet its "duty to report provision of the HIA". This purpose is discussed further below, as part of legal and regulatory compliance.

[100] I considered this submission, but was not persuaded by it. Despite the assertion that date of birth is required so that the Symptom Checker does not inappropriately suggest a screening test, ultimately screening tests are discussed and reviewed between an individual and their health care provider. Therefore, if the Symptom Checker suggested a screening test that an individual was not eligible for, a health care provider would provide recommendations regarding testing and appropriate timelines. The same would apply in the case of prescribing medications, in which case a health care provider or pharmacist would be directly involved and would be in the best position to advise as to the specifics of what medications can or cannot be taken by an individual of a specific age.

**Findings**

- It is reasonable for Babylon to require users to respond to questions in order to provide its Symptom Checker and Healthcheck services (non-medical AI-generated general health information). It is reasonable to collect information about age and gender for these purposes.
- It is not reasonable for Babylon to collect full date of birth for these purposes. Babylon's collection and use of personal information for this purpose does not meet the requirements of sections 11 and 16 of PIPA to collect and use personal information for reasonable purposes and only to the extent that is reasonable.

**Recommendation**

- I recommend that Babylon discontinue the collection and use of full date of birth within the Symptom Checker function.

***Providing Clinical Services***

[101] As previously described, app users are able to book Clinical Services appointments (consultations) with physicians, dietitians, and mental health counsellors. The information collected, used and disclosed as part of consultations with dietitians and mental health counsellors is personal information subject to PIPA, although identifiable information associated with consultations with physicians is health information that is subject to HIA.[12]

*Government-Issued Identification and Selfie Photo*

[102] When an individual books an appointment with a dietitian or mental health counsellor through the app, the individual is required to provide a photo of their government-issued ID as well as a selfie photo as part of making the appointment.

[12] See Investigation Report H2021-IR-01.

[103] With respect to this practice, the "What personal data we hold and how we get it" section of Babylon's Privacy Policy says:

> When you register with us, you complete forms and provide us with basic information about yourself, such as your name, date of birth, physical address and email address. **You will also provide us with a copy of identification documentation for ID checks to be carried out on our behalf by one of our service providers**... [emphasis added]

[104] Babylon's Privacy Policy does not provide any further information about the collection of this information or how it is used. I asked Babylon for additional information and was advised as follows:

> 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.

[105] In my view, the collection of government-issued ID and a selfie photo "before an appointment is booked" is beyond what is reasonable for Babylon's purpose of verifying identity.

[106] I acknowledge that when providing Clinical Services to an individual, Babylon needs to ensure it has properly identified the individual. I also acknowledge that there may be some incidence of fraud whereby patients submit false information in order to access treatment. Babylon did not, however, provide any evidence to indicate the prevalence of this problem, such that it would be reasonable to require every individual making an appointment for Clinical Services consultations to provide government-issued ID and a selfie photo.

[107] 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.

[108] From this, I understand Babylon is describing the use of a facial recognition technology, which, in my view, represents the collection and use of particularly sensitive personal information which should only occur when there is a reasonable purpose and only to the extent to meet that purpose.[13]

[109] Outside of the Babylon by TELUS Health app, if an individual were to make an appointment with a dietitian or mental health counsellor for an in-person consultation, the individual would typically call ahead, give their name, describe the purpose for seeking a consultation, and make an appointment. The individual would not be required to provide a copy of government-issued ID or a selfie photo at the time of booking the appointment. This seems to me to be an unreasonable collection, particularly if the individual cancels the appointment, at which point Babylon would have collected this sensitive information for no purpose at all.

[110] Upon actually attending an in-person appointment, an individual might be required to verify their identity by producing government-issued ID to be viewed. However, it is unlikely the Practitioner would collect a copy of that ID or a selfie photograph or use facial recognition technology to verify identity, or that it would be reasonable to do so.

[111] In my view, Babylon's purpose can be accomplished by asking the individual to show government-issued ID to the camera at the time of the consultation, as is commonly done with in-person consultations. In the event the consultation is by telephone, the Practitioner could ask the individual to confirm certain pieces of information (date of birth) before proceeding, as is a common practice when providing financial services by telephone. It is not reasonable for Babylon to collect more information than an individual would reasonably be required to provide, merely because the individual is participating in an online consultation.

[112] I note my finding is also consistent with several OIPC orders, as well as investigation reports, related to the collection and retention of identification documents.[14]

[113] After being advised of my finding, Babylon made an additional submission where it argued that its identity verification process was "critically important for the provision of healthcare delivered in the virtual care context". It stated that there are…

> …significant qualitative differences between the delivery of healthcare in-person and the virtual care context. In an in-person setting, the provider (or more often their staff) can easily verify identity by looking at the identity document and comparing it to the individual in front of them. This is much more difficult to do on screen when someone is holding an ID up to a camera, and

[13] 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.

[14] See Orders P2012-010, P2007-015 and P2007-016, and P2021-IR-01.

> physicians simply do not have the skill set to do this effectively. In person, the staff can also hold the document to validate its authenticity, which is not possible to do online. Further, the risk of fraud in the online context is greater (see, for example, Forbes article titled: ["Fighting Telemedicine Fraud: Why Robust Verification Is Needed"]…

[114] Babylon also disagreed with the comparison to financial services providers for telephone consultations, saying:

> [F]inancial services providers collect extensive personal information from customers, which thereafter can be used to authenticate the individual on an ongoing basis. Babylon practitioners do not have sufficient information about the user to do this effectively (for example, validating name, contact information and/or date of birth alone (single factor authentication) is not, on its own, a sufficiently robust identity verification mechanism for establishing a relationship to obtain healthcare services). Moreover, in addition to the authentication issues explained above, requiring users to show their ID to the camera at the time of the consultation is also inefficient and can lead to delays or appointment cancellations (for example, if the user is not able to locate their ID at the outset of the appointment). In sum, Babylon considers this identity verification process crucial to the delivery of safe patient care and the detection and prevention of fraud, and, accordingly, cannot discontinue its use.

[115] I did not find this submission to be persuasive. For the various reasons outlined in this report, and with no additional compelling arguments to the contrary, I maintain my findings and recommendations with regard to the collection of government-issued ID and selfie photographs. In addition, and as I have outlined in the Babylon HIA report, I have found overwhelming evidence to support identity verification being accomplished in ways that do not involve the collection and use of this personal information.[15] Furthermore, the OIPC has reviewed and accepted numerous PIAs, to date, for virtual care applications that do not collect copies of ID or selfie photos of its users. This demonstrates that it is possible as well as practical to avoid collecting this information while still providing virtual care services to individuals.

**Finding**

- Collecting some personal information in order to verify identity and detect and prevent fraud is reasonable; however, collecting and using a copy of government-issued identification and a selfie photograph is beyond what is reasonable for these purposes. Therefore, Babylon has not met the requirements of sections 11 and 16 of PIPA to collect and use personal information for reasonable purposes and only to the extent that is reasonable, particularly as it appears Babylon is using a facial recognition technology to verify identity "before an appointment is booked".

[15] See Investigation Report H2021-IR-01.

**Recommendation**

- I recommend that Babylon discontinue the collection and use of government-issued identification and selfie photograph.

***"Health and Medical Information"***

[116] During a virtual consultation, dietitians and mental health counsellors employed by Babylon collect personal information from individuals. As previously noted, the "What personal data we hold and how we get it" section of the Privacy Policy says:

> The main type of information we hold about you is health and medical information: information about your health, symptoms, treatments, test results, consultations and sessions, medications and procedures. This includes details of your consultations with our doctors...

[117] The "What we use your personal data for" section of the Privacy Policy 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. It may also include **sharing information with other healthcare professionals as necessary for the provision of care to you**, such as your GP, specialist referral services, therapists, pharmacists, hospitals, accident and emergency services, pathology service providers, and diagnosis centres chosen by you **for the purpose of imaging request forms**. It may also include Babylon physicians and their designates accessing your medical and / or prescription history contained within provincial databases (including but not limited to, PharmaNet, NetCare, Drug Profile Viewer) **for the purpose of providing care or for the purpose of monitoring medication use**. [emphasis added]

[118] The "Sharing your personal data with others" section of the Privacy Policy says:

> We will, **where necessary for your treatment or care**, share your information with your other health and social care providers. For example, your GP, specialist referral services, therapists, pharmacists, hospitals, accident and emergency services, pathology service providers, diagnosis centers chosen by you for the purpose of imaging requests, and other health and care bodies... [emphasis added]

[119] In my view, it is reasonable for Babylon to collect, use and disclose identifying personal information ("health and medical information") during the course of providing Clinical Services consultations with dietitians and mental health counsellors, for the purposes of providing medical diagnosis, healthcare or treatment, and monitoring medication use.

**Finding**

- Collecting, using and disclosing personal information ("health and medical information") in order to provide medical diagnosis, healthcare or treatment, and monitoring medication use is reasonable and in accordance with sections 11, 16 and 19 of PIPA.

***Recording Consultations***

[120] At the time this investigation was initiated, individuals had the option to record their consultations with a dietitian or mental health counsellor. With respect to this practice, the "What personal data we hold and how we get it" section of Babylon's Privacy Policy says the following under "Health and medical information":

> We retain recordings of our consultations and interactions with you. This can include your use of our digital tools, such as chatbot, Healthcheck and monitoring services, video and audio recordings or audio-only recordings. This is in order to provide you with an easy way to check your consultations where you wish to, so that we can ensure high quality care is provided to you, and, with your consent, to allow us to learn from them to improve our services…

[121] 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. [emphasis added]

[122] In my view, Practitioners recording consultations by taking notes in order to provide "medical diagnosis, and the provision of healthcare or treatment" is consistent with typical practices when similar services are provided in-person, and is a reasonable extent of collection. It is not clear to me, however, why Babylon would retain a video or audio recording of the consultation for these purposes, given the Practitioner would also make notes of the encounter and record that information in Babylon's electronic medical record.

[123] In response to my concern, Babylon provided additional information, saying:

> The recording functionality implemented by Babylon is entirely optional and is initiated only after explicit consent is provided by the patient (in real time at the start of the consultation). A recording serves two wholly reasonable and important purposes that benefit patients, specifically (i) recordings are used for quality control purposes, and (ii) a recording enhances the patient record and can be accessed by the patient upon request.

[124] I found this submission to be persuasive, particularly given Babylon's assertion that "recording functionality implemented by Babylon is entirely optional and is initiated only after explicit consent is provided by the patient (in real time at the start of the consultation)". I note, however, that when I downloaded the app during this investigation to understand this functionality, it appeared Babylon was relying on opt-out consent and not "explicit consent". Given Babylon's reassurance in this submission, however, I find that collecting, using and retaining audio and video recordings of sessions with mental health counsellors and dietitians is reasonable for enhancing the patient record, provided appropriate consent is obtained from individuals.[16]

[16] Babylon's collection of recordings for quality control purposes is discussed later in this report.

[125] This finding differs from my finding in Investigation Report H2021-IR-01 with respect to health custodians and the collection, use and retention of audio and video recordings. HIA requires that custodians limit their collection and use of health information to what is "essential" to meet the custodian's purpose. HIA does not contemplate that a custodian can collect non-essential health information, even with patient consent.

**Finding**

- Collecting, using and retaining audio and video recordings of consultations with mental health counsellors and dietitians is reasonable for the purpose of "enhanc[ing] the patient record" and meets the requirements of sections 11 and 16 of PIPA to collect and use personal information for reasonable purposes and only to the extent that is reasonable, provided appropriate consent is obtained from the individual.

***Location Data***

[126] The "What we use your personal data for" section of the Privacy Policy describes Babylon's collection and use of location data 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.

[127] Babylon provided the following information to explain why it collects location data:

> In our view, it is entirely reasonable to offer users (on an express consent basis) a tool that uses location data to help them find a nearby pharmacy. Moreover, the fact that dietitians and mental health counsellors have limited ability to write prescriptions is not relevant, as they may nevertheless recommend other products available at a pharmacy, including supplements, health products and foods.

[128] Despite the fact dietitians and mental health counsellors "have limited ability to write prescriptions", Babylon explained that the information is collected as they "may nevertheless recommend other products available at a pharmacy, including supplements, health products and foods". Given this information, I accept that Babylon has a reasonable purpose for collecting precise location data to direct individuals to the nearest pharmacy (as described in the Privacy Policy), provided appropriate consent is obtained from individuals. Babylon cannot, however, require individuals to provide this information and there must be an opportunity for individuals to disable or prevent collection of precise location information.

[129] The purpose for which Babylon "derives" approximate location from IP address is not clear from either the Privacy Policy or Babylon's submission. It is also not clear whether the derivation (collection) is with consent. If this information is "derived" from IP

address for the purpose of directing individuals to the nearest pharmacy, Babylon has not explained why it would be reasonable to collect this additional information when it already collects precise location with consent. Given this, I find the collection and use of approximate location is not reasonable for this purpose.

[130] I note that my finding that it is reasonable to collect precise location with consent does not extend to the services provided by physicians (custodians) under HIA.[17] The threshold for collecting and using health information under HIA is that the information must be "essential" to meet the custodian's purpose.

**Findings**

- It is reasonable for Babylon to collect precise location information for the purpose of dietitians and mental health counsellors directing individuals to the nearest pharmacy. This collection and use of personal information meets the requirements of sections 11 and 16 of PIPA to collect and use personal information for reasonable purposes and only to the extent that is reasonable, provided the collection is not made mandatory and the app provides the opportunity for individuals to consent to the collection.
- Deriving (collecting) approximate location from IP address is not reasonable for the purpose of directing individuals to the nearest pharmacy, given Babylon already collects precise location with consent.

***Billing and Payment***

[131] The "What personal data we hold and how we get it" section of the Privacy Policy says the following under the subheading "Financial Information":

> If you make any payments on the App, your credit/debit card details are processed directly by a third party processor that will store all payment information and transaction details. We will only retain details of transactions on secure servers and we will not retain your credit or debit card information.

[132] The "Sharing your personal data with others" section of the Privacy Policy says:

> We may share your personal information with companies we have hired to provide services on our behalf, such as ... billing and payment processing...
>
> Where you access our services through public or private health insurance, and where you have given your consent, we will need to let your insurance company know your name, email address, policy number, location (based on IP address), demographic information, that you had an appointment with us, the date of the appointment, details of your diagnosis, prescription, pharmacy location, whether or not you had a referral made and other similar information about your appointment with us

[17] Please see Investigation Report H2021-IR-01 for the discussion of collection of location data under HIA.

[133] In addition to the above, Babylon's Terms and Conditions document provides additional information about "Price and Payment".

[134] In my view, it is reasonable for Babylon to collect, use and disclose financial information (including credit/debit card details) for the purposes of processing payment for billable services (i.e. where the user pays). It is also reasonable for Babylon to disclose identifying information such as name, email address, policy number, location, demographic information, and appointment information to an individual's insurance company in order for the latter to process a claim, although I note the Privacy Policy does not specifically identify this as the purpose for which this information may be disclosed.[18]

**Findings**

- Babylon's collection, use and disclosure of personal financial information (including credit or debit card details) in order to obtain payment for billable services is for reasonable purposes and to a reasonable extent, in accordance with sections 11, 16 and 19 of PIPA.
- It is reasonable for Babylon to disclose name, contact information and appointment details to an individual's insurance company in order for the latter to process a claim (provided Babylon obtains consent. See discussion of consent below).

***Technical Services Support***

[135] The "What personal data we hold and how we get it" section of Babylon's Privacy Policy says:

> To monitor our service quality, we may retain records of when you contact our support teams via email or phone.

[136] This section of the Privacy Policy also says the following with respect to "Technical information and analytics":

> When you use our App or visit our website, we may automatically collect the following information where this is permitted by your device or browser settings:
>
> (a) technical information, including the address used to connect your mobile phone or other device to the Internet, your login information, system and operating system platform type and version, device model, browser or app version, time zone setting, language and location preferences, wireless carrier and your location (based on IP address); and

[18] The Privacy Policy in place at the start of this investigation did not identify the purpose for which Babylon "will need to let your insurance company" know certain personal information about users. However, the Privacy Policy was later revised to say that this information would be provided to insurance companies, with consent, for purposes of processing a claim.

(b) information about your visit (such as when you first used the App and when you last used it, and the total number of sessions you have had on that App), including products and services you viewed or used, App response times and updates, interaction information (such as button presses or the times and frequency of your interactions with the communications we deliver to you in the App or otherwise) and **any phone number used to call our customer service number**. [emphasis added]

[137] The "What we use your personal data for" section of the Privacy Policy says the following , under "Other uses":

> Based on our legitimate interest in managing and planning our business, we may analyse data about your use of our products and services to, for example, **troubleshoot bugs** within the App or our website… [emphasis added]

[138] The "Sharing your personal data with others" section of the Privacy Policy says:

> We have partnered with TELUS Health to provide certain services on our behalf, including **technical and customer support** and communications. Your personal data will be shared with TELUS Health as necessary to allow TELUS Health to provide these services to you and to us...
>
> We may share your personal information with companies we have hired to provide services on our behalf, such as **data hosting and processing**, **technical support**, billing and payment processing, marketing and communications... [emphasis added]

[139] From the above excerpts, I understand that Babylon automatically collects technical information about a user's mobile phone or other device used to access the app, as well as about a user's interactions with the app, and interactions with customer service for the purposes of providing technical and customer support, troubleshooting, and data hosting and processing.

[140] The Privacy Policy is not clear exactly why this much detailed information is collected or at what points when a user interacts with the app. It is also not clear if this "technical information" is included in the general category of "personal data" that is shared with TELUS Health, acting on Babylon's behalf, to provide "customer support".

[141] In particular, I am concerned that the Privacy Policy says "technical information" – including device model, wireless carrier and IP address – and information about interactions is automatically collected where "permitted by your device or browser settings", presumably from the moment a user downloads the app. This suggests the app is collecting more information than is reasonable to meet its purposes.

[142] In response to this concern, Babylon provided additional information, stating:

> The technical information collected by the app is basic technical information that most apps and other digital services collect. This is not, in any way, unusually "detailed information". There are sound and entirely compelling operational and security reasons for collecting this information. For example, IP addresses are basic information used to identify abuse, attacks, and generally suspect, fraudulent behaviour and would be more concerning if not collected. Other information, such as information about a user's device and operating system, is required in order to technically deliver the

app and to deliver content appropriate for the device's capabilities. The Privacy Policy is clear that the technical information is collected "when you use our App or visit our website". In sum, Babylon cannot discontinue the collection and use of this technical information.

[143] Based on this additional information, I accept that collecting IP address and other information about a user's device and operating system is reasonable for the purposes Babylon has identified. I note, however, that Babylon did not provide an explanation for its collection of information about an individual's wireless carrier. Given this, I find that collection of wireless carrier information is not reasonable.

**Finding**

- It is reasonable for Babylon to collect some personal information from individuals, including IP address and device information, in order to provide technical services support, troubleshooting and data hosting and processing. However, Babylon's automatic collection and use of information regarding an individual's wireless carrier is beyond what is reasonable for these purposes and does not meet the requirements of sections 11(2) and 16(2) of PIPA to collect and use personal information only to the extent that is reasonable for meeting the purposes for which the information is collected or used.

**Recommendation**

- I recommend that Babylon discontinue the automatic collection and use of individuals' wireless carrier information.

***Legal and Regulatory Compliance***

[144] The "What we use your personal data for" section of the Privacy Policy describes a number of "Other uses" for which Babylon collects, uses and discloses personal information, including:

> We also store your medical information, such as notes from consultations, recordings of our consultations with you as well as your interactions with our digital services ... for **safety, regulatory, and compliance purposes**. For example, we may need to review your information and, where necessary, **make disclosures in compliance with lawful requests by regulatory bodies or as otherwise required by law or regulation**.
>
> **Where necessary for safety, regulatory and/or compliance purposes**, we may audit consultations and your other interactions with our services. Strict confidentiality and data security provisions will apply at all times to any such audit and access. [emphasis added]

[145] The "Sharing your personal data with others" section of the Privacy Policy includes a section called "Information sharing with other healthcare providers" which says that Babylon…

> ...will, where necessary for your treatment or care, share your information with your other health and social care providers. For example... other health and care bodies. This may include sharing information with such services for safeguarding purposes in accordance with our legal or professional obligations.
>
> We may preserve or disclose information about you to comply with a law, regulation, legal process, or governmental request; to assert legal rights or defend against legal claims; or to prevent, detect, or investigate illegal activity, fraud, abuse, violations of our terms, or threats to the security of our services or the physical safety of any person.

[146] I accept that it is reasonable that some personal information (including "medical information" collected via Clinical Services consultations) might be used and disclosed by Babylon "for safety, regulatory, and compliance purposes" or as "otherwise required by law or regulation". I note that the Privacy Policy does not specify exactly what personal information might be used or disclosed for these purposes, but I assume it would depend to some extent on the nature of said requests or requirements arising in the future, and it is impossible to know in advance what all of those might be.

[147] Collecting the least amount of identifiable information in the first place, and then using and disclosing the least amount of identifiable information to meet legal and regulatory purposes as they arise would be reasonable and, with this in mind, I recommend that the Privacy Policy include specific language addressing the basic privacy principle of data minimization when using or disclosing personal information for these purposes.

[148] In addition to the above, I note that when I asked Babylon about the purpose for which it collects date of birth from individuals when they interact with the app's Symptom Checker function, I was told:

> As stated in a previous response, collection of date of birth determines eligibility and also it is a useful, specific identifier in the event of an issue. For example, if one of our clinicians spotted a user entering symptoms for 'someone else' were suggestive of abuse (e.g non-accidental injury) we would want a way to identify the individual at risk if we needed to investigate this/report it under the duty to report provision of the HIA.

[149] I understand this statement to mean that Babylon collects date of birth when individuals interact with the Symptom Checker digital health tool because this information might be required "in the event of an issue" and if an investigation was required "under the duty to report provision of the HIA".

[150] I note that HIA does not include any "duty to report provision" and, in any event, does not apply to the collection, use or disclosure of information through the Symptom Checker tool, given that no health service is provided by a custodian. Further, Babylon did not provide any information to suggest that it is monitoring individuals' use of the Symptom Checker function in real time, or to explain how it would use this information in a timely way "in the event of an issue". Given this, Babylon has not demonstrated that it is reasonable to collect this sensitive identifying information from every user of

Symptom Checker for this speculative purpose. I note also that none of Babylon's public-facing documents identify this as a purpose for collecting personal information.

**Finding**

- The use and disclosure of some personal information (including "medical information" collected via Clinical Services consultations) for legal and regulatory compliance purposes is reasonable, and complies with sections 16 and 19 of PIPA.
- It is not reasonable to collect date of birth from every user of Symptom Checker "in the event of an issue" or in case an investigation is warranted at some future time. Therefore, collection of this sensitive information for this speculative future purpose does not meet the requirement of section 11 of PIPA to collect personal information for reasonable purposes and only to the extent that is reasonable**.**

**Recommendation**

- I recommend that Babylon's Privacy Policy include specific language addressing the basic privacy principle of data minimization when first collecting identifiable information, and then using or disclosing identifiable personal information for these secondary legal and regulatory purposes.
- I recommend that Babylon discontinue collecting date of birth information within its Symptom Checker service.

***Quality Improvement***

[151] With respect to "Technical information and analytics", the "What personal data we hold and how we get it" section of Babylon's Privacy Policy says:

> When you use our App or visit our website, we may automatically collect the following information where this is permitted by your device or browser settings:
>
> (a) technical information, including the address used to connect your mobile phone or other device to the Internet, your login information, system and operating system platform type and version, device model, browser or app version, time zone setting, language and location preferences, wireless carrier and your location (based on IP address); and
>
> (b) information about your visit (such as when you first used the App and when you last used it, and the total number of sessions you have had on that App), including products and services you viewed or used, App response times and updates, interaction information (such as button presses or the times and frequency of your interactions with the communications we deliver to you in the App or otherwise) and **any phone number used to call our customer service number**.
>
> We work with partners who provide us with **analytics** and advertising services (for our services only and not for third party advertising). This includes **helping us understand how users interact with our services**, providing our advertisements on the internet, and **measuring performance of our services and our adverts**. Cookies and similar technologies may be used to collect this information, such as

> your interactions with our services. You can change your device settings to block cookies, or to notify you before a cookie is set. If you block cookies, you may not be able to use all the features of our App. You can prevent the setting of cookies by adjusting the settings on your browser or your mobile phone. [emphasis added]

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

> Where you have provided your explicit consent, we will use your medical information (always having removed personal identifiers, such as your name, address and contact details) to **improve our healthcare products and services, and our artificial intelligence system, so that we can deliver better healthcare to you and other Babylon users**. This medical information (with your personal identifiers removed in the way described above) may include your medical record (both records received and created by us), transcripts and recordings of your consultations, and your interactions with our artificial intelligence services, such as our symptom checker and other digital tools. This does not involve making any decisions which would have a significant effect on you – **it is only about improving our products, services and software so that we can deliver a better experience to you and other Babylon users, and help achieve our aim of making healthcare affordable and accessible to everyone**. Strict confidentiality and data security provisions apply at all times. This consent relates to information that can identify you. [emphasis added]

[153] This section of the Privacy Policy also describes a number of "Other uses" for which Babylon collects, uses and discloses personal information, including:

> Based on our legitimate interest in managing and planning our business, we may analyse data about your use of our products and services to, for example, ... forecast demand of service and to **understand other trends in use, including which features users use the most and find most helpful, and what features users require from us**. This does not involve making any decisions about you that would have a significant legal effect on you – it is **only about improving our App so that we can deliver better services to you**. Strict confidentiality and data security provisions will apply at all times. [emphasis added]

[154] The "Sharing your personal data with others" section of the Privacy Policy says:

> We share personal data (with identifiers removed) with members of our corporate group to help us **develop, improve and maintain our software and artificial intelligence system** (where you have explicitly consented to this use of your data). [emphasis added]

[155] Babylon's Privacy Policy describes the automatic collection of a significant amount of information about a user's mobile phone or other device used to access the app, as well as about a user's interactions with the app, and interactions with customer service. The Privacy Policy is not overly clear as to the purpose for which the information is collected; however, a subsequent paragraph says, "We work with partners who provide us with **analytics** and advertising services..." [emphasis added]

[156] I understand this to mean that technical information and information about interactions with the app is collected and used, at least in part, for quality improvement purposes. Other paragraphs in the Privacy Policy suggest that information that is used to "improve our healthcare products and services" is de-identified; however, it is not always clear that this is the case. For example, the same paragraph that suggests technical information is used for analytics also says it is used for advertising purposes, which

seemingly would require identifying information. The Privacy Policy also says that where users provide "explicit consent", Babylon will use medical information "to improve our healthcare products and services, and our artificial intelligence system, so that we can deliver better healthcare to you and other Babylon users". This suggests the information is identifiable thus requiring consent, but also says "always having removed personal identifiers, such as your name, address and contact details". Similarly, in a later submission, Babylon said that it records consultations "for quality control purposes", but it is not clear how this aligns with the Privacy Policy statement that, "This medical information (with your personal identifiers removed in the way described above) may include… recordings of your consultations".

[157] Overall, the Privacy Policy is not clear what identifiable personal information is collected for quality improvement purposes. In my view, the various paragraphs of the Privacy Policy suggest that Babylon is collecting more identifiable personal information than is reasonable to meet this purpose.

[158] In response to this concern, Babylon provided the following additional information:

> Babylon takes a privacy by design approach to its use of user information for quality improvement purposes, including by using pseudonymized or anonymized data where practicable to do so. However, it is entirely reasonable for Babylon to use personal information for these purposes.
>
> (1) It is critical to the safety and effectiveness of the app that Babylon's Clinical Safety team have the ability to access and use personal information in order to audit and validate the safety and effectiveness of the service.
>
> (2) With respect to training Babylon's algorithms and improving the digital health tools, Babylon has implemented an entirely reasonable process whereby it offers users the choice by way of express consent to allow Babylon to use their medical information - with all personal identifiers removed - for quality improvement purposes. Consistent with companies across all sectors, including the health sector, Babylon uses this data to create, improve and offer innovative and effective digital health tools to users.
>
> (3) Consistent with widespread and wholly legitimate practices of companies across all sectors, Babylon uses technical information to improve its product and services. These practices are entirely reasonable and in fact critical to Babylon's ability to effectively and safely provide its digital health care tools and services.

[159] I reviewed and considered the additional information provided by Babylon, which consists mainly of asserting and reasserting that its practices are "entirely reasonable" and "critical", without explaining why this is the case. I am not persuaded by Babylon's arguments that "companies across all sectors" have the same practices. Overall, I maintain my finding that it is not clear what identifiable personal information is collected for quality improvement purposes and the various paragraphs of the Privacy Policy suggest that Babylon is collecting more identifiable personal information than is reasonable to meet this purpose. Babylon did not provide any compelling reasons for collecting and using identifying personal information – rather than de-identified information – for quality improvement purposes.

**Finding**

- Babylon has not provided any compelling reasons for collecting and using identifying information for quality improvement purposes. As such, this collection and use is beyond what is reasonable for the purpose and does not meet the requirements of sections 11(2) and 16(2) of PIPA to collect and use personal information only to the extent that is reasonable for meeting the purposes for which the information is collected or used.

**Recommendation**

- I recommend that Babylon discontinue the collection and use of identifying personal information for quality improvement purposes.

***Marketing and Communications***

[160] Section 2 of Babylon's Privacy Policy ("What personal data we hold and how we get it") says, "When you register with us, you complete forms and provide us with basic information about yourself, such as your name, date of birth, physical address and email address".

[161] This section of the Privacy Policy does not say for what purpose a user's name and contact information is collected, although the "Keeping you up to date" portion of the "What we use your personal data for" section says:

> We use your email address, phone number and/or details to contact you or present you with occasional updates and marketing messages where you have not opted out, based on our legitimate interest in marketing our services to you and subject to your right to opt out at any time.
>
> As part of providing you with high quality preventative and occupational health care services, we may contact you by SMS, email and/or other means to offer you helpful information or invite you to make appointments, for example for free healthcare screening programmes (such as cervical cancer screening).

[162] In addition, the "Sharing your personal data with others" section of the Privacy Policy says:

> We have partnered with TELUS Health to provide certain services on our behalf, including technical and customer support and **communications**. Your personal data will be shared with TELUS Health as necessary to allow TELUS Health to provide these services to you and to us. With your consent, we will also share your personal data, such as name and contact details (but not medical or health data) with TELUS Health so that TELUS Health can tell you about their products or services that might be of interest to you.
>
> We may share your personal information with companies we have hired to provide services on our behalf, such as ...marketing and communications. [emphasis added]

[163] In my view, collecting, using and disclosing basic contact information such as email address and telephone number is reasonable for communications purposes, including offering "helpful information" and sending "occasional updates and marketing messages". However, this collection, use and disclosure can only be deemed to be reasonable if consent is obtained from the individual.

**Finding**

- Collecting, using and disclosing basic contact information such as email address and telephone number is reasonable for marketing and communications purposes, including offering "helpful information" and sending "occasional updates and marketing messages", and complies with sections 11(2), 16(2) and 19(2)of PIPA, provided Babylon obtains consent. See discussion of consent below.

## Issue 3: Does Babylon notify individuals of the purpose(s) for which personal information is collected, as required by section 13 of PIPA?

[164] Section 13 of PIPA says:

> **Notification required for collection**
>
> 13(1) Before or at the time of collecting personal information about an individual from the individual, an organization must notify that individual in writing or orally
>
> (a) as to the purposes for which the information is collected, and
> (b) of the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection.

[165] Babylon notifies individuals of the purposes for which personal information is collected by means of its Terms and Conditions and Privacy Policy.

***Terms and Conditions and Privacy Policy***

[166] When an individual first downloads the app, they see a "Sign up" page with a statement that says, "By proceeding you acknowledge that you have read and agree to the Terms & Conditions". The Terms and Conditions generally describes the services the app provides, and other information technical requirements, pricing and liability.

[167] Sections C, L and M of the Terms and Conditions refer users to Babylon's Privacy Policy saying, for example, "Our use of your personal information is governed by our Privacy Policy" and "Our Privacy Policy sets out how your personal information will be used by us".[19]

[168] At the end of the Terms and Conditions, individuals can select "Agree" or "Disagree".

[169] Below the Terms and Conditions statement on the app's Sign-up page, is another statement that says, "Use of Babylon by TELUS Health is subject to the Privacy Policy". The Privacy Policy is linked from this statement. As previously discussed, the Privacy Policy generally describes the personal information Babylon collects, and the purposes for which it is collected, used and disclosed. The beginning of the Privacy Policy includes the following statement:

> If you have any questions about how we process your information, please don't hesitate to get in touch by contacting our Privacy Officer at privacyofficer@babylonhealth.com.

[19] "(C) WHAT WE NEED FROM YOU IN ORDER TO PROVIDE SERVICES", "(L) HOW WE MAY USE YOUR PERSONAL INFORMATION", and "(M) CONSULTATION RECORDINGS"

[170] A similar statement is found at the end of the Privacy Policy:

> For any questions or concerns, or if you'd like information about how to lodge a complaint with us or an applicable privacy commissioner's office, you can contact us by sending an email to privacyofficer@babylonhealth.com.

[171] Having reviewed the Terms and Conditions and Privacy Policy, I make the following observations.

*Length and Readability*

[172] As described, both the Terms and Conditions and the Privacy Policy are linked from the sign-up page, which users see as soon as they download the app.

[173] The Terms and Conditions document is approximately 14-15 pages in 11-point font, and is 6,500+ words in length. The Privacy Policy is approximately 7 pages long in 11-point font, and almost 3,000 words in length.

[174] These linked documents are intended to be viewed by users accessing them via mobile devices.

[175] In my view, however, the length of these documents and the primary means of accessing them (mobile device) makes it unlikely users will have a reasonable understanding of the purposes for collection "Before or at the time of collecting personal information" as specified in section 13(1) of PIPA. As a result, they will not be aware of the purposes for which personal information is collected and used, particularly those that are not obvious (such as analytics, marketing and communications, etc.). Many users will not, at the time of downloading the app, ever read the 3,000-word Privacy Policy.

*Information Collected and Purpose for Collection*

[176] The Privacy Policy includes seven sections, including "What personal information we hold and how we get it" (section 2), "What we use your personal information for" (section 3), and "Sharing your personal information" (section 4).

[177] Although these sections provide significant detail about what personal information is collected and the purposes for which it is collected, used and disclosed, I found the purposes do not align with the subheadings in the document and are not easily discernable. Further, it is not always clear what information is collected for what purpose. For example, section 2 of the Privacy Policy says:

> When you register with us, you complete forms and provide us with basic information about yourself, such as your name, date of birth, physical address and email address. You will also provide us with a copy of identification documentation for ID checks to be carried out on our behalf by one of our service providers, and health card number/provincial health insurance number for the purposes of us

> billing the public health system. You are responsible for the accuracy of the information that you provide to us.

[178] There is no other information in the Privacy Policy that explains why an individual would have to provide "basic information about yourself" including physical address and email address in order to register for the app. This gap is not addressed in any other sections of the Privacy Policy. It is possible that the physical address is collected to verify residency requirements for a Clinical Services consultation, or possibly for communications purposes. It may be that email address is collected at the sign-up stage for marketing/communications purposes, but this is also not clear as the paragraph starts, "When you register with us, you... provide us with basic information...".

[179] It is also not clear why this paragraph says, "When you register with us" you "will provide" a copy of ID documents "for ID checks". It appears this is actually required only when an individual makes an appointment for a Clinical Services consultation. Further, I earlier noted my concern that, based on a submission Babylon provided for this investigation, it appears Babylon uses a facial recognition technology in order to verify the identity of every user who makes an appointment for a Clinical Services consultation. This identity verification purpose and use of a particularly sensitive technology is not described anywhere in Babylon's Privacy Policy or within the app itself.

[180] Another example concerns the section of the Privacy Policy that describes the technical information collected by the app automatically when "permitted by your device or browser settings", including information about interactions with and uses of the app generally. While the descriptions are quite detailed and lengthy, the next paragraph says, "We work with partners who provide us with **analytics** and **advertising** services (for our services only and not for third party advertising)" [emphasis added]. It is not clear what information is collected for analytics, and what information is collected for advertising.

[181] Further, this and other paragraphs in the Privacy Policy suggest that information that is used to "improve our healthcare products and services, and our artificial intelligence system, so that we can deliver better healthcare to you and other Babylon users" is de-identified, but it is not clear that this is always the case. The same paragraph that suggests technical information is used for analytics also says it is used for advertising purposes, which seemingly would require identifying information. The Privacy Policy also says that users "provide... explicit consent" so Babylon can "improve our healthcare products and services", which suggests the information is identifiable and therefore requires consent, but also says "always having removed personal identifiers".

[182] One last example from the Privacy Policy (as discussed above with respect to Location Data):

> 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.

[183] This paragraph is clear that precise location is collected, with consent, for the purpose of directing an individual to the nearest pharmacy. However, it is not clear why "approximate location" is collected, why it would be necessary to collect approximate location (particularly if precise location has been collected), or whether approximate location is collected and used with consent.

[184] These are just a few examples to illustrate the lack of clarity with respect to what information is collected for what purpose(s).

*Inconsistencies Between Privacy Policy and App Implementation*

[185] There are a number of inconsistencies between the information collection practices described in the Privacy Policy and the actual implementation of the app. For example, the Privacy Policy says:

> When you register with us, you complete forms and provide us with basic information about yourself, such as your name, **date of birth**, physical address and email address. [emphasis added]

[186] In reality, when an individual first registers for the app, the sign-up page prompts them to provide first and last name, email address, street address, and postal code, and create a password. Individuals are not prompted to provide date of birth at the time they register for the app.

[187] Similarly, in a number of places, the Privacy Policy describes collection, use and disclosure practices for functions that are not available. For example, the Privacy Policy says:

> We may also hold information about you and your health from other apps, devices and services where you have given your consent to that data being shared with us. Examples include where you decide to share information collected from a smart watch or similar device with our App.

[188] I asked Babylon to provide additional information about the types of apps, devices, and services used to send health information to Babylon, as well as the consent obtained for sharing that data. Babylon advised me that, "This reference within the Privacy Policy relates to a service that will be available to our Canadian users in June 2020".

[189] Another example concerns the use of social media logins. Babylon's Privacy Policy says:

> You may choose to connect your existing accounts with other providers (such as a social media provider), for example, when signing up to make it easier to create an account with us. If you choose to do this, we will receive limited information about you from that provider, such as your email address and name. Provided we are acting in accordance with data protection laws, we may also use information from other sources, such as specialist companies that supply information, online media channels, our commercial partners and public registers. This information can for example, help us to improve and measure the effectiveness of our services.

[190] The integration of applications with social media authentication mechanisms presents additional risks to the privacy of personal information, including increased risk of compromise and the reduced ability for individuals to know if their login information has been misused. I asked Babylon to explain what types of authentication options are available, details around each type of authentication, and a list of all providers that can be used to authenticate.

[191] In response, Babylon advised that "The Babylon by TELUS Health app currently does not have this feature enabled. Babylon does not enable social or single sign-ons from any other provider for end users." Babylon added to this after their review of the draft investigation report, stating that "The Babylon by TELUS Health app is not and never was integrated with social media."

[192] Finally, in one last example, the Privacy Policy says:

> The main type of information we hold about you is health and medical information: information about your health, symptoms, treatments, test results, consultations and sessions, medications and procedures. This includes details of your consultations with our doctors, and interactions with our digital services, including interactions with our chatbot, symptom checker, 'Ask a doctor', Healthcheck, Digital Twin services, health monitoring, or other health and condition management services. **Your interactions with our digital services may be shared with our doctors in order to provide you with a better experience and for the purposes of providing you health care**. [emphasis added]

[193] I asked Babylon Health whether physicians are able to view the information as described in the Privacy Policy and was told "no".

[194] In my view, the references in the Privacy Policy to collection of information through functionality that is not yet enabled or available within the Babylon application are misleading and potentially confusing to Babylon's users.

[195] Overall, I find that because of the above issues related to length and readability, the lack of clarity with respect to what information is collected for what purpose(s), and inconsistencies between the Privacy Policy and implementation of the app, Babylon has not met the requirements of section 13 of PIPA.

[196] I understand that Babylon's position is that "this finding fails to recognize in any way the steps that Babylon took to comply with section 13".

[197] Nonetheless, I reiterate my finding. It is a fundamental principle of privacy that an organization should inform individuals about the purposes for which it is collecting personal information at the time of the collection. This information should be available with reasonable effort on the part of the individual and in a form that is generally understandable. For the reasons discussed above, I find Babylon has not met this legal requirement.

**Finding**

- Babylon's Privacy Policy does not meet the requirements of section 13 of PIPA to notify individuals of the purpose(s) for which personal information is collected. It is unlikely individuals will understand the purposes for collection from the lengthy linked documents viewed via their small screen mobile devices. Further, the Privacy Policy does not clearly identify the purposes for which personal information is collected, nor what information is associated with what purpose. In addition, the Privacy Policy included significant inaccurate information related to functionality that is not yet enabled or available.

  Due to these issues, individuals may not adequately understand the purposes for which Babylon collects personal information during the individual's use of the app.

**Recommendation**

- I recommend that Babylon update the Privacy Policy, to correct any inaccurate statements as well as reduce the length of the document. In addition, an in-app notification added to the app would provide an additional method to notify individuals using the app of the purposes for which Babylon collects personal information.

## Issue 4: Does Babylon use service providers outside Canada to collect, use, disclose or store personal information for or on its behalf? If so, has Babylon met the requirements of sections 6 and 13.1 of PIPA with respect to developing policies and practices and notifying individuals?

[198] Section 6 of PIPA reads as follows:

> **Policies and practices**
>
> 6(1) An organization must develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act.
>
> (2) If an organization uses a service provider outside Canada to collect, use, disclose or store personal information for or on behalf of the organization, the policies and practices referred to in subsection (1) must include information regarding
>
> (a) the countries outside Canada in which the collection, use, disclosure or storage is occurring or may occur, and
> (b) the purposes for which the service provider outside Canada has been authorized to collect, use or disclose personal information for or on behalf of the organization.
>
> (3) An organization must make written information about the policies and practices referred to in subsections (1) and (2) available on request.
>
> …
>
> **Notification respecting service provider outside Canada**
>
> 13.1(1) Subject to the regulations, an organization that uses a service provider outside Canada to collect personal information about an individual for or on behalf of the organization with the consent of the individual must notify the individual in accordance with subsection (3).
>
> (2) Subject to the regulations, an organization that, directly or indirectly, transfers to a service provider outside Canada personal information about an individual that was collected with the individual's consent must notify the individual in accordance with subsection (3).
>
> (3) An organization referred to in subsection (1) or (2) must, before or at the time of collecting or transferring the information, notify the individual in writing or orally of
>
> (a) the way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada, and
> (b) the name or position name or title of a person who is able to answer on behalf of the organization the individual's questions about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization.
>
> (4) The notice required under this section is in addition to any notice required under section 13.

[199] With respect to its service providers, Babylon UK said:

> 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.
>
> Access to data by Babylon Partners Limited is only granted in accordance with Babylon's information governance framework (namely by named and role-based access). Selected staff at Babylon Partners Limited may access data in order to troubleshoot technical issues for the service....

Babylon UK also advised that, "The Babylon platform uses selected third-party service providers in order to offer a telemedicine service". Babylon UK reported it uses service providers for the following purposes:

- 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 [Telus service]
- Email
- Technical analytics & performance
- Identification validation
- On-call support
- eFaxes
- Application messaging
- Testing
- Marketing
- Voice conferencing and SMS
- Video conferencing
- Clinical support

[200] I asked Babylon to provide details regarding the location of their service providers. Babylon provided the following information:

- Ireland
- Europe, the Middle East and Africa
- UK
- Global Google infrastructure
- USA
- Canada

[201] As noted previously, sections 6 and 13.1 of PIPA say that where an organization uses a service provider outside of Canada to collect, use, disclose or store personal information, the organization's policies and practices **must include information regarding:**

- **the countries** in which personal information is collected, used, disclosed or stored, and
- **the purposes for which the service provider outside of Canada has been authorized to collect, use or disclosure personal information.**

[202] Before or at the time the organization collects or transfers the personal information to a service provider outside of Canada, the organization must:

- Notify the individual of how they may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada, and
- Notify the individual of the name or position name or title of a person who is able to answer questions about the collection, use, disclosure or storage of personal information by service providers outside Canada.

[203] With respect to service providers outside of Canada, Babylon's Privacy Policy says:

> Your data may be processed stored or accessed by Babylon or our service providers from inside or outside of Canada, including in the European Union. In either case, personal data will be protected in accordance with data protection law and subject to strict safeguards. For example, when we do transfer personal data outside of Canada, we strive to minimize the amount of personal data that we transfer. Notwithstanding these safeguards, while outside of Canada, personal data may be accessible by foreign government agencies under applicable law.

[204] Although the Babylon Privacy Policy says that, "Your data may be processed stored or accessed by Babylon or our service providers from inside or outside of Canada", it does not include information regarding the countries in which personal information is collected, used, disclosed or stored, and the purposes for which the service provider(s) outside of Canada are authorized to collect, use or disclose personal information, as required by section 6(2) of PIPA.

[205] The Privacy Policy does say:

> For any questions or concerns, or if you'd like information about how to lodge a complaint with us or an applicable privacy commissioner's office, you can contact us by sending an email to privacyofficer@babylonhealth.com.

[206] In my view, however, this paragraph does not meet the requirement under section 13.1(3) of PIPA to advise individuals "before or at the time of collecting or transferring the information" of "the way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside of Canada" and to provide contact information for a person who is

able to answer questions "about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization".

[207] With respect to the above concerns, Babylon advised as follows:

> PIPA does not require that detailed information about service providers be included in the outward facing Privacy Policy. In fact, the OIPC wrote the following to Babylon on November 14, 2020: While it is not a requirement to proactively disclose a table of all the service providers and the related data elements to individuals, for the sake of transparency, it is good practice to list the specific countries where personal information transits through/is stored.
>
> PIPA does not require that the Privacy Policy state verbatim: "for information about the organization's policies and practices with respect to service providers outside of Canada, contact….". Rather, relevant contact information must be provided, which Babylon has done.

[208] It is true that PIPA does not require an organization to "proactively disclose a table of all the service providers and the related data elements to individuals". However, PIPA does require organizations to notify individuals "of how they may obtain access to written information about the organization's policies and practices with respect to service providers outside Canada" and those policies and practices must include information about "the countries" in which personal information is collected, used, disclosed or stored, and "the purposes" for which the service provider outside of Canada has been authorized to collect, use or disclosure personal information. Section 13.1(4) specifically says that "The notice required under this section is **in addition to any notice required under section 13**" [emphasis added].

[209] Given this, I do not accept that providing a general email address that individuals can use to contact Babylon "For any questions or concerns" meets the requirement in section 13.1(3). I also do not accept that the Privacy Policy statement that, "Your data may be processed stored or accessed by Babylon or our service providers from inside or outside of Canada, including in the European Union" meets the requirement in section 6(1) and (2) to develop policies and procedures that include information regarding the countries outside Canada in which the collection, use disclosure or storage occurs and the purposes for which the service provider outside Canada has been authorized to collect, use or disclose personal information. If Babylon has such policies and procedures, it has failed to produce them to me during this investigation.

**Findings**

- Babylon engages services providers outside of Canada, including Ireland, Europe, the Middle East, Africa, the UK and the USA.
- Babylon has not developed policies and practices that include information regarding the countries in which personal information is collected, used, disclosed or stored, and the purposes for which service provider(s) outside of Canada are authorized to collect, use or disclose personal information, as required by section 6(2) of PIPA.

- Babylon has not met the requirement under section 13.1(3) of PIPA to advise individuals "before or at the time of collecting or transferring the information" of "the way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside of Canada" and to provide contact information for a person who is able to answer questions "about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization".

**Recommendations**

- I recommend that Babylon develop policies and practices that include information regarding the countries in which personal information is collected, used, disclosed or stored, and the purposes for which service provider(s) outside of Canada are authorized to collect, use or disclose personal information.
- I recommend that Babylon update its Privacy Policy to advise individuals "before or at the time of collecting or transferring the information" of "the way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside of Canada" and to provide contact information for a person who is able to answer questions "about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization".

## Issue 5: Does Babylon collect, use and disclose personal information with consent (unless otherwise authorized), as required by section 7 of PIPA?

[210] Section 7(1) of PIPA requires organizations to obtain consent from individuals for the collection, use or disclosure of personal information, except where the Act provides otherwise. Section 7(1) of PIPA states:

> **Consent required**
>
> 7(1) Except where this Act provides otherwise, an organization shall not, with respect to personal information about an individual,
>
> (a) collect that information unless the individual consents to the collection of that information,
> (b) collect that information from a source other than the individual unless the individual consents to the collection of that information from the other source,
> (c) use that information unless the individual consents to the use of that information, or
> (d) disclose that information unless the individual consents to the disclosure of that information.Section 8 of the *Health Information Regulation* sets out additional security requirements including:

[211] The various forms of consent are described in section 8 of PIPA as follows:

> **Form of consent**
>
> 8(1) An individual may give his or her consent in writing or orally to the collection, use or disclosure of personal information about the individual.
>
> (2) An individual is deemed to consent to the collection, use or disclosure of personal information about the individual by an organization for a particular purpose if
>
> (a) the individual, without actually giving a consent referred to in subsection (1), voluntarily provides the information to the organization for that purpose, and
> (b) it is reasonable that a person would voluntarily provide that information....
>
> (3) Notwithstanding section 7(1), an organization may collect, use or disclose personal information about an individual for particular purposes if
>
> (a) the organization
>
> (i) provides the individual with a notice, in a form that the individual can reasonably be expected to understand, that the organization intends to collect, use or disclose personal information about the individual for those purposes, and
> (ii) with respect to that notice, gives the individual a reasonable opportunity to decline or object to having his or her personal information collected, used or disclosed for those purposes,
>
> (b) the individual does not, within a reasonable time, give to the organization a response to that notice declining or objecting to the proposed collection, use or disclosure, and
> (c) having regard to the level of the sensitivity, if any, of the information in the circumstances, it is reasonable to collect, use or disclose the information as permitted under clauses (a) and (b).

[212] I reviewed the Babylon Privacy Policy and specific areas within the app where personal information is collected, used and disclosed. I also reviewed the "Health Information Flows Table" provided by Babylon UK, which describes some of Babylon's legal authorities for collecting, using and disclosing personal and health information for various purposes under PIPA and HIA respectively.

[213] Given the many functions of the app, the complex data flows, and certain issues with the Privacy Policy, I found it was not feasible to verify Babylon's authority for each and every collection, use and disclosure of personal information. Nonetheless, I make the following observations.

***Section 8(1) – Express Consent***

*Policies and Procedures*

[214] The form of consent described in section 8(1) of PIPA is sometimes referred to as "express" or "explicit" consent – that is, an individual expressly consents to the collection, use or disclosure of personal information for a particular purpose. Babylon says it relies on section 8(1) of PIPA for its authority to collect and use some personal information via the app.

[215] For example, sections of the Privacy Policy say:

- "Where you have provided your explicit consent, we will use your medical information (always having removed personal identifiers, such as your name, address and contact details) to improve our healthcare products and services, and our artificial intelligence system, so that we can deliver better healthcare to you and other Babylon users... This consent relates to information that can identify you."
- "We share personal data (with identifiers removed) with members of our corporate group to help us develop, improve and maintain our software and artificial intelligence system (where you have explicitly consented to this use of your data)."

[216] When I asked Babylon to clarify its consent practices, Babylon said:

> Affirmative action (sliding the consent toggle or selecting 'Sure') is required by the user to indicate consent. If they do not take this affirmative step, they are deemed to have not consented. Users can re-visit the app and amend this consent setting at any time in the Privacy Controls section within the app.

[217] Babylon gave the same response with respect to its authority to collect personal information from individuals using the Symptom Checker and Healthcheck tools.

[218] I understand Babylon's response to mean that it considers that a user who has agreed to the Privacy Policy and slides the consent toggle (or selects "Sure" or "Got it") has expressly consented to the collection and use of personal information for specific purposes.

[219] In my view, however, this combination of actions is not express consent as contemplated by section 8(1) of PIPA for a number of reasons (some of which were previously discussed in Issue 3 above). For example:

- Users must click on a link to read a 7-page, 3,000-word Privacy Policy, likely using a small screen mobile device.
- The Privacy Policy does not clearly identify the purposes for which personal information is collected or what personal information is collected for what purpose, and it includes inaccurate information (e.g. refers to functionality that is not implemented).
- The Privacy Policy describes Babylon's practices in a number of sections (e.g. "When you provide your optional explicit consent, we use data to build a better Babylon....") but is not itself a consent statement.
- The Privacy Policy conflates a number of different purposes and does not indicate which collections and uses of personal information are integral to providing a service, and which are optional.

[220] Given all of the above, it is not at all clear what a user is agreeing to when they click "Got it" or "Sure", such that this action could be considered an express consent as contemplated by section 8(1) of PIPA.

[221] When providing consent, individuals must understand what they are consenting to. The length and readability issues with the Privacy Policy and Terms and Conditions may be prohibitive to users obtaining this understanding. Investigation Report P2020-IR-01[20] addresses the issue of consent and in that report, the OIPC (and other jurisdictions) recommended that users be provided with a prominent notice to describe the purposes where personal information is collected and used, particularly where the purposes are not obvious to the user. To address this issue, I recommend that Babylon provide an in-app summary of the purposes for which it collects and uses personal information.

[222] The "Health Information Flows" table that Babylon UK provided for this investigation also says Babylon relies on section 8(1) for authority to collect and use government issued ID in order to "verify identity".

[223] I downloaded the app and noted that, when individuals choose to make an appointment with a Practitioner for Clinical Services, they see a screen that says, "Before you start... we just need a few details. It won't take long". Two options are provided:

- "Verify your identity. Use your passport or another ID."
- "Add your details. This helps us give you the best care."

[224] If the user selects "Verify your identity", they will see a screen that says, "Please verify your ID to ensure that we can prescribe medication and discuss your medical history

[20] See Investigation Report P2020-IR-01.

with you". If the individual clicks on "Verify Now", a pop-up is displayed that says "Babylon by TELUS Health Would Like to Access the Camera" and "Enable your camera in settings". Presumably, this is so that the individual can provide a selfie photograph to the app.

[225] In my view, providing government-issued ID and a selfie photo in these circumstances is not an express consent as contemplated by section 8(1) of PIPA, given the user does not actually give a consent to the collection and use of this information for specific purposes.

[226] Further, as I earlier noted, I understand that Babylon uses a facial recognition technology in order to verify the identity of users prior to making an appointment for a consultation. This purpose and use of this sensitive technology is not described anywhere in Babylon's Privacy Policy or within the app itself. Therefore, it cannot be said that individuals have expressly consented to the collection of their personal information for this purpose.

***Section 8(2) – Deemed Consent***

[227] Section 8(2) of PIPA says an individual is "deemed to consent" to the collection, use or disclosure of personal information "for a particular purpose" if the individual "without actually giving a consent... voluntarily provides the information to the organization for that purpose" and "it is reasonable that a person would voluntarily provide that information".

[228] In my view, there are a number of transactions that occur where an individual provides personal information voluntarily while using the app, which could be authorized by virtue of deemed consent. For example, users of the app's non-medical digital tools (Symptom Checker and Healthcheck) voluntarily provide information in response to AI-generated questions in order to receive "general medical information on the types of conditions that people who have experienced similar symptoms have had" (Symptom Checker), or "a report based on general statistical information of certain diseases and conditions" (Healthcheck). Various statements displayed by the app at the time the user engages with these functions make it obvious why the information is collected, despite the absence of an express consent statement ("I consent to..."). In my view, it is reasonable that individuals would voluntarily provide answers to the questions, such that they will receive the general medical information or reports.

[229] If this information were to be used for purposes other than generating "general medical information" or the Healthcheck report, however, Babylon could not rely on deemed consent as individuals would not be voluntarily providing personal information for these specific purposes (that is, the purposes are not obvious).

[230] Further, I reiterate my earlier finding that although it is reasonable for Babylon to collect some identifiable information, such as name and email address, it is not reasonable to

collect physical address and postal code to provide these non-medical digital healthcare services in the first place. Even if Babylon were to obtain deemed consent (or any other form of consent), this alone is not a silver bullet; organizations are required to establish reasonable purposes for collecting, using and disclosing personal information and ensure the extent of collection is reasonable to meet those purposes. Individuals cannot consent to an unreasonable purpose.

[231] Another example where Babylon says it relies on deemed consent is when users sign-up or register for the app. That is, the "Health Information Flows" table provided by Babylon UK for this investigation specifically says that Babylon relies on section 8(2) to authorize the "transfer" of personal information (email, password and user ID) to a third party service provider for "account verification". I take this to mean that Babylon relies on deemed consent to collect and use personal information for this purpose.

[232] While it is true that individuals voluntarily provide information and are prompted to create a password when they first land on the sign-up page, in my view the purposes are not obvious. That is, Babylon has advised that this information is collected for the "establishment of a secure account and contractual relationship with an individual", to "allow users to maintain records of their interactions", to "allow for this more holistic and personalized offering", and for "user safety purposes" (so Babylon can "contact users who are demonstrating concerning activity on the Symptom Checker"). In my view, none of these purposes are obvious, such that Babylon can rely on deemed consent to collect and use the information.

[233] The "Health Information Flows" table also says that Babylon relies on section 8(2) to authorize the following "transfers" of personal information to third party service providers for the stated purposes:

- Name and email address to Third Party to facilitate email communications
- Name and email address to Third Party to facilitate marketing communications
- Name, email address, registration date, address, gender, date of birth to Third Party to send marketing and informational communications

[234] These specific personal information data elements (with the exception of gender and date of birth) are collected at the sign-up stage. There is nothing about the sign-up page that would lead users to understand that they are providing this information for email, marketing and informational communications, such that the information could be said to be collected with deemed consent.

[235] Finally, I will note that one of the criteria for reliance on section 8(2) deemed consent is that it must be reasonable that an individual would voluntarily provide personal information for a specific purpose, despite the individual not expressly saying "I consent to the collection of..."

[236] In my view, Babylon cannot rely on section 8(2) for the collection of information such as gender and date of birth for the purpose of "sending marketing and informational communications" as it is not reasonable that an individual would voluntarily provide this information for this purpose. Similarly, Babylon's collection of government-issued ID and a selfie photograph to verify identity (as discussed in the preceding section on express consent) cannot be authorized by deemed consent, given the personal information in question and because it appears Babylon is relying on facial recognition technology behind the scenes, without explicitly saying so. This purpose and use of personal information is not obvious to individual users.

***Section 8(3) – Opt-out Consent***

[237] Section 8(3) of PIPA describes an "opt-out" form of consent. That is, where an organization provides easy-to-understand notice to the individual of the particular purposes for the collection, use or disclosure, and the individual has a reasonable opportunity to decline or object, and opt-out consent is appropriate for the level of sensitivity of the personal information involved.

[238] In addition to transactions that appear to rely on express and deemed consent, I noted at least one example where Babylon asserts it obtains section 8(1) (express) consent, when in fact it appears to rely on section 8(3) consent.

[239] When this investigation was initiated in April 2020, users had the ability to choose to record their interactions with Practitioners. Babylon's Privacy Policy says that these interactions are recorded with consent, and noted, "There is a consent toggle in the app which allows patients to opt in or out of consultation recordings. Additionally, physicians are asked to check this consent prior to a consultation."

[240] I downloaded the app and observed that when an individual books an appointment with a Practitioner they see a screen that includes a "Preferences" section that says, "You can choose for your consultation to be recorded. This allows our clinical management team to audit the quality of our service. You'll be asked again during your appointment, in case you change your mind".

[241] This option is accompanied by a toggle switch. The default for this toggle switch is "On". That is, users must actively choose not to have their consultation recorded.

[242] In my view, this does not qualify as an "express" consent as contemplated by section 8(1) of PIPA in that, should the individual do nothing, they are assumed to have consented to the recording of their consultation. It is also not a deemed consent as contemplated by section 8(2) of PIPA, as the individual does not voluntarily provide any information.

[243] Instead, it appears to be an "opt-out" consent, in that Babylon has provided notice that the consultation will be recorded to allow "our clinical management team to audit the

quality of our service". The individual can use the toggle switch to decline or object to the collection.

[244] Despite the appearance of a section 8(3) consent, I note that one of the criterion for opt-out consent is that "having regard to the level of the sensitivity, if any, of the information in the circumstances, it is reasonable to collect, use or disclose the information" with notice and providing the individual with an opportunity to opt-out or decline. In my view, given the sensitivity of recorded consultations with dietitians and mental health counsellors, this criterion has not been met.

[245] Another example where Babylon appears to rely on opt-out consent is with respect to the collection and use of technical information and information about a user's interactions with the app. Babylon's Privacy Policy says:

> When you use our App or visit our website, we may **automatically collect the following information** where this is permitted by your device or browser settings:
>
> (a) technical information, including the address used to connect your mobile phone or other device to the Internet, your login information, system and operating system platform type and version, device model, browser or app version, time zone setting, language and location preferences, wireless carrier and your location (based on IP address); and
>
> (b) information about your visit (such as when you first used the App and when you last used it, and the total number of sessions you have had on that App), including products and services you viewed or used, App response times and updates, interaction information (such as button presses or the times and frequency of your interactions with the communications we deliver to you in the App or otherwise) and any phone number used to call our customer service number.

[246] Despite the fact that the collection of this information is addressed in the Privacy Policy, there is no indication, based on the statement, "When you use our App or visit our website, we may automatically collect the following information", that individuals are provided with a reasonable opportunity to decline or object to this collection and use. Instead, the Privacy Policy concludes with a button the user can click to indicate "Got it" (in other cases, the Privacy Policy is accompanied by a button the user can click to indicate "Sure").

[247] Furthermore, in my view, the Privacy Policy does not contain adequate detail that would provide a clear understanding to individuals regarding why this information is collected or used and for what purpose. For these reasons, I find that Babylon has not obtained consent for the collection and use of this information.

***Disclosure vs. Transfer to a Third-Party Service Provider***

[248] As previously noted, Babylon's Privacy Policy and its submissions for this investigation make reference to both "transfers" of personal information and "disclosures" of personal information. Overall, I found these references suggest Babylon may not be clear as to its obligations under PIPA for obtaining consent.

[249] For example, the "Health Information Flows" table provided by Babylon UK for this investigation says that Babylon relies on section 8(2) (deemed consent) in a number of situations, including to authorize the following "transfers" of personal information to third parties:

- Email, password and user ID to Third Party for account verification
- Credit card number, name, billing address to Third Party in order to process payments
- Name and email address to Third Party to facilitate email communications
- Name and email address to Third Party to facilitate marketing communications
- Name, email address, registration date, address, gender, date of birth to Third Party to send marketing and informational communications.

[250] Pursuant to section 5(2) of PIPA, where an organization engages the services of a person (a third party service provider), whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with this Act.

[251] That is, if Babylon engages a service provider to collect personal information on Babylon's behalf, for a particular purpose, Babylon is generally required to obtain consent for that collection and use. However, Babylon is not required to obtain consent specifically for the engagement of or transfer to the third party. Therefore, when Babylon says it relies on deemed consent (section 8(2)) for authority to transfer personal information to third parties for processing, I have understood this to mean Babylon relies on deemed consent for the collection and use of personal information for specific purposes for which the third party has been engaged.

[252] A clear example where Babylon will require consent to disclose information to a third party is with respect to insurance companies. With respect to this disclosure, Babylon's Privacy Policy says the following:

> Where you access our services through public or private health insurance, and where you have given your consent, we will need to let your insurance company know your name, email address, policy number, location (based on IP address), demographic information, that you had an appointment with us, the date of the appointment, details of your diagnosis, prescription, pharmacy location, whether or not you had a referral made and other similar information about your appointment with us.

[253] I asked Babylon to provide me with information regarding the consent process for the disclosure of personal information to third parties, such as insurance companies. Babylon provided the following response:

> Babylon's Clinical Operations team have not dealt [with] a query of this nature yet, however, would expect to obtain consent in this instance and for such consent to be recorded.

[254] Should Babylon have to deal with such a query in future, it will be required to obtain consent. I recommend Babylon obtain express consent (section 8(1) of PIPA) for the disclosure of such sensitive information to insurance companies.

[255] Overall, I find that Babylon's consent practices do not comply with the requirements set out in PIPA, for a variety of reasons. Babylon responded to my concerns by saying the following:

> With respect to express consent, while Babylon welcomes feedback from the OIPC to improve the clarity and readability of the Privacy Policy, it disagrees with the OIPC's finding that the Privacy Policy presented – in full text - and accepted by users cannot constitute valid consent. Regardless, where the Babylon Privacy Policy states that express consent is obtained, a real time in-app express consent is obtained and Babylon does not rely only on the acceptance of the privacy policy, contrary to what is suggested by the findings in the Draft Report.

[256] With respect to deemed consent, Babylon said:

> With respect to account creation and authentication, and marketing and communications, these are all purposes that are obvious to and reasonably expected by users of digital services. The purpose for collecting government issued ID and selfie is clearly described to the user and deemed consent is entirely appropriate given the nature of the technology used in connection with Babylon's identity verification process.

[257] With respect to opt-out consent, Babylon said:

> With respect to consent for audio and video recordings, Babylon strongly disagrees that the process in place at the outset of the investigation constituted opt-out consent. While the in-app toggle was defaulted to "on", the user was again asked at the outset of the consultation whether they wanted the consultation recorded, which constitutes express consent. In essence, this was a double consent, with the first being opt-out and the second (and determinative consent) being express opt-in.
>
> Babylon's process for obtaining consent for the collection and use of technical information is entirely reasonable and consistent with industry practice.

[258] In response to these submissions, I note that while there may be some examples of in-app express consents, I reiterate my previous comments that because of the length, readability, lack of clarity and inaccuracies in the Privacy Policy, Babylon cannot rely on the combination of its Privacy Policy and the consent toggle for express consent. I reviewed the Privacy Policy in detail, repeatedly, and found it difficult to understand Babylon's information handling practices for the reasons it stated. In my view, Babylon cannot assume users understand the purposes for which personal information is collected such that they could be said to be providing express consent when they select "sure" or "got it".

[259] With regard to account creation and authentication, and marketing and communications, I reject Babylon's submission that these purposes are obvious to and reasonably expected by users of digital services. It is not obvious at the registration/sign-up page that the purpose for collecting personal information is to

establish “a secure account and contractual relationship with an individual”, to “allow users to maintain records of their interactions” and to “allow for this more holistic and personalized offering”. These purposes were only articulated to me through Babylon’s submissions during this investigation. Babylon’s customer-facing materials do not explain how the Babylon service offering differs from free services, such that identifying information is needed. It is also not clear in the Privacy Policy or sign-up page that personal information is collected “to contact users who are demonstrating concerning activity on the Symptom Checker (e.g., suicidal tendencies or signs of being victims of domestic violence”. It cannot be said that these purposes are obvious, such that individuals provide deemed consent when they register.

[260] In particular, it is not clear from the Privacy Policy or the in-app experience that Babylon is using facial recognition technology to identify individuals. It is my view that, particularly when using such a technology, as well as out-of-country service providers, and sensitive information such as a facial biometric, the onus is on Babylon to be completely transparent about its practices. As these factors are not obvious, it cannot be said that users provide deemed consent to the collection and use of their personal information for the purpose of identification.

[261] With respect to obtaining consent for audio and video recordings, I note that Babylon acknowledges that the “first consent” is in fact an opt-out consent, not an express consent as described in the Privacy Policy (Babylon says that it has now changed this). Babylon asserts that the “second (and determinative consent)” is the one that matters, and is an express opt-in. As I did not engage in an actual consultation with a Practitioner, I am not able to verify the second, express consent.

[262] And finally, with respect to its reliance on opt-out consent for the collection and use of technical information, Babylon asserts this “is entirely reasonable and consistent with industry practice”. I do not find this statement to be persuasive as it does not address my previous finding that there is no indication that individuals are provided with a reasonable opportunity to decline or object to this collection and use, which is a requirement of opt-out consent under PIPA. I also reiterate my previous comment that the Privacy Policy does not contain adequate detail to provide a clear understanding to individuals regarding why this information is collected or used and for what purpose. For these reasons, I find that Babylon has not obtained consent for the collection and use of this information.

**Findings**

- Babylon's consent practices do not comply with the requirements set out in PIPA for the following reasons:

    - Babylon cannot rely on the combination of its Privacy Policy and the consent toggle for express consent as the Privacy Policy is linked, lengthy, lacking clarity, and contains inaccurate information.
    - Deemed consent may be appropriate in some circumstances; however, there are numerous examples where it appears the purposes for the collection may not be obvious, and it may not be reasonable that a user would voluntarily provide information for specified purposes. Relying on deemed consent is particularly inappropriate when Babylon collects and uses government-issued identification and a selfie photograph for purposes of verifying identity, and more so given that Babylon is not transparent about the technology and process it is using.
    - Where Babylon wishes to rely on opt-out consent, it must provide easy to understand notice and a clear opportunity to opt-out. This option will not usually be appropriate when sensitive information is at issue.
    - Babylon's Privacy Policy and submissions for this investigation suggest Babylon is not clear as to its consent obligations under PIPA when transferring information to third party service providers versus disclosing information to third parties.

    Babylon has not met the requirements of section 7 of PIPA with respect to obtaining consent for collection, use and disclosure of personal information, unless otherwise authorized.

## Summary of Findings

[263] My findings from the investigation are:

- Babylon collects, uses and discloses personal information for eight general purposes:
    - Sign-up / registration
    - Providing non-medical digital healthcare services (including Symptom Checker and Healthcheck)
    - Providing Clinical Services (including medical diagnosis, healthcare and treatment, and prescribing and monitoring medication)
    - Billing and payment
    - Technical services support (including hosting, troubleshooting, and managing and processing data)
    - Legal and regulatory compliance (including fraud detection and prevention)
    - Quality improvement (including analytics to improve products, services, software; and "develop, improve and maintain ... software and artificial intelligence system")
    - Marketing and communications (including sending updates and marketing communications)

- Babylon has a reasonable purpose for collecting and using name and email address when an individual signs-up/registers for the app.

- Babylon has not demonstrated that it is reasonable to collect personal information at the registration stage for user safety purposes.

- The collection of physical address and postal code goes beyond what is reasonable for Babylon's stated purposes. Therefore, Babylon has not met the requirements of sections 11 and 16 of PIPA to collect personal information only to the extent that is reasonable for meeting its purposes.

- It is reasonable for Babylon to require users to respond to questions in order to provide its Symptom Checker and Healthcheck services (non-medical AI-generated general health information). It is reasonable to collect information about age and gender for these purposes.

- It is not reasonable for Babylon to collect full date of birth for its Symptom Checker service (non-medical AI-generated general health information). Babylon's collection and use of personal information for this purpose does not meet the requirements of sections 11 and 16 of PIPA to collect and use personal information for reasonable purposes and only to the extent that is reasonable.

- Collecting some personal information in order to verify identity and detect and prevent fraud is reasonable; however, collecting and using a copy of government-

issued identification and a selfie photograph is beyond what is reasonable for these purposes. Therefore, Babylon has not met the requirements of sections 11 and 16 of PIPA to collect and use personal information for reasonable purposes and only to the extent that is reasonable, particularly as it appears Babylon is using a facial recognition technology to verify identity "before an appointment is booked".

- Collecting, using and disclosing personal information ("health and medical information") in order to provide medical diagnosis, healthcare or treatment, and monitoring medication use is reasonable and in accordance with sections 11, 16 and 19 of PIPA.

- Collecting, using and retaining audio and video recordings of consultations with mental health counsellors and dietitians is reasonable for the purpose of "enhanc[ing] the patient record" and meets the requirements of sections 11 and 16 of PIPA to collect and use personal information for reasonable purposes and only to the extent that is reasonable, provided appropriate consent is obtained from the individual.

- It is reasonable for Babylon to collect precise location information for the purpose of dietitians and mental health counsellors directing individuals to the nearest pharmacy. This collection and use of personal information meets the requirements of sections 11 and 16 of PIPA to collect and use personal information for reasonable purposes and only to the extent that is reasonable, provided the collection is not made mandatory and the app provides the opportunity for individuals to consent to the collection.

- Deriving (collecting) approximate location from IP address is not reasonable for the purpose of directing individuals to the nearest pharmacy, given Babylon already collects precise location with consent.

- Babylon's collection, use and disclosure of personal financial information (including credit or debit card details) in order to obtain payment for billable services is for reasonable purposes and to a reasonable extent, in accordance with sections 11, 16 and 19 of PIPA.

- It is reasonable for Babylon to disclose name, contact information and appointment details to an individual's insurance company in order for the latter to process a claim (provided Babylon obtains consent).

- It is reasonable for Babylon to collect some personal information from individuals, including IP address and device information, in order to provide technical services support, troubleshooting and data hosting and processing. However, Babylon's automatic collection and use of information regarding an individual's wireless carrier is beyond what is reasonable for these purposes and does not meet the

requirements of sections 11(2) and 16(2) of PIPA to collect and use personal information only to the extent that is reasonable for meeting the purposes for which the information is collected or used.

- The use and disclosure of some personal information (including "medical information" collected via Clinical Services consultations) for legal and regulatory compliance purposes is reasonable, and complies with sections 16 and 19 of PIPA.

- It is not reasonable to collect date of birth from every user of Symptom Checker "in the event of an issue" or in case an investigation is warranted at some future time. Therefore, collection of this sensitive information for this speculative future purpose does not meet the requirement of section 11 of PIPA to collect personal information for reasonable purposes and only to the extent that is reasonable**.**

- Babylon has not provided any compelling reasons for collecting and using identifying information for quality improvement purposes. As such, this collection and use is beyond what is reasonable for the purpose and does not meet the requirements of sections 11(2) and 16(2) of PIPA to collect and use personal information only to the extent that is reasonable for meeting the purposes for which the information is collected or used.

- Collecting, using and disclosing basic contact information such as email address and telephone number is reasonable for marketing and communications purposes, including offering "helpful information" and sending "occasional updates and marketing messages", and complies with sections 11(2), 16(2) and 19(2)of PIPA, provided Babylon obtains consent.

- Babylon's Privacy Policy does not meet the requirements of section 13 of PIPA to notify individuals of the purpose(s) for which personal information is collected. It is unlikely individuals will understand the purposes for collection from the lengthy linked documents viewed via their small screen mobile devices. Further, the Privacy Policy does not clearly identify the purposes for which personal information is collected, nor what information is associated with what purpose. In addition, the Privacy Policy included significant inaccurate information related to functionality that is not yet enabled or available.

  Due to these issues, individuals may not adequately understand the purposes for which Babylon collects personal information during the individual's use of the app.

- Babylon engages services providers outside of Canada, including Ireland, Europe, the Middle East, Africa, the UK and the USA.

- Babylon has not developed policies and practices that include information regarding the countries in which personal information is collected, used, disclosed or stored,

and the purposes for which service provider(s) outside of Canada are authorized to collect, use or disclose personal information, as required by section 6(2) of PIPA.

- Babylon has not met the requirement under section 13.1(3) of PIPA to advise individuals "before or at the time of collecting or transferring the information" of "the way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside of Canada" and to provide contact information for a person who is able to answer questions "about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization".

- Babylon's consent practices do not comply with the requirements set out in PIPA for the following reasons:

    - Babylon cannot rely on the combination of its Privacy Policy and the consent toggle for express consent as the Privacy Policy is linked, lengthy, lacking clarity, and contains inaccurate information.
    - Deemed consent may be appropriate in some circumstances; however, there are numerous examples where it appears the purposes for the collection may not be obvious, and it may not be reasonable that a user would voluntarily provide information for specified purposes. Relying on deemed consent is particularly inappropriate when Babylon collects and uses government-issued identification and a selfie photograph for purposes of verifying identity, and more so given that Babylon is not transparent about the technology and process it is using.
    - Where Babylon wishes to rely on opt-out consent, it must provide easy to understand notice and a clear opportunity to opt-out. This option will not usually be appropriate when sensitive information is at issue.
    - Babylon's Privacy Policy and submissions for this investigation suggest Babylon is not clear as to its consent obligations under PIPA when transferring information to third party service providers versus disclosing information to third parties.

    Babylon has not met the requirements of section 7 of PIPA with respect to obtaining consent for collection, use and disclosure of personal information, unless otherwise authorized.

## Summary of Recommendations

[264] Based on my findings from and during this investigation, I recommend that Babylon:

- Modify its registration process to eliminate the requirement for individuals to provide physical address and postal code at the time an individual registers for the app.

- Discontinue the collection and use of full date of birth within the Symptom Checker function.

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

- Discontinue the automatic collection and use of individuals' wireless carrier information.

- Update its Privacy Policy to include specific language addressing the basic privacy principle of data minimization when first collecting identifiable information, and then using or disclosing identifiable personal information for these secondary legal and regulatory purposes.

- Discontinue the collection and use of identifying personal information for quality improvement purposes.

- Update the Privacy Policy, to correct any inaccurate statements as well as reduce the length of the document. In addition, an in-app notification added to the app would provide an additional method to notify individuals using the app of the purposes for which Babylon collects personal information.

- Develop policies and practices that include information regarding the countries in which personal information is collected, used, disclosed or stored, and the purposes for which service provider(s) outside of Canada are authorized to collect, use or disclose personal information.

- Update its Privacy Policy to advise individuals "before or at the time of collecting or transferring the information" of "the way in which the individual may obtain access to written information about the organization's policies and practices with respect to service providers outside of Canada" and to provide contact information for a person who is able to answer questions "about the collection, use, disclosure or storage of personal information by service providers outside Canada for or on behalf of the organization".

## Closing Comments

[265] 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.

[266] 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.

[267] 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:

- "Privacy Commitment that includes more detail about the purposes for which registration information is collected and used."
- "[I]mplemented a new Privacy Commitment with enhanced transparency around the collection and use of identifiable information for Symptom Checker and Healthcheck. In addition, TELUS Health MyCare's new Privacy Commitment includes more detail about the purposes for which the date of birth will be used in symptom checker."
- "[I]mplemented a new Privacy Commitment and a set of FAQs that provide a clear explanation of the manner in which ID is verified using government-issued identification and a selfie photo."
- "The "toggle" to consent to audio consultations within the app is now set to "off". Additionally, as was the case at the start of the investigation, express consent is also collected verbally during the consultation with a healthcare practitioner."
- "[I]mplemented a new Privacy Commitment and Code that specifically address and commits to data minimization throughout TELUS Health MyCare's data handling lifecycle."
- "[I]mplemented a new Privacy Commitment as well as an FAQ, which offers users both a summary and detailed level view of its personal information practices."
- "[I]mplemented an internal Standard of Practice (SOP) that includes the documentation of information regarding the countries in which personal information is collected, used, disclosed or stored, and the purposes for which service provider(s) outside of Canada are authorized to collect, use or disclose personal information. In addition, TELUS Health MyCare has implemented a new Privacy Commitment that further enhances transparency on the use of service providers outside of Canada."
- "[I]mplemented a new Privacy Commitment that provides contact details for an individual who can answer questions about the manner in which TELUS Health MyCare or its service providers treat Personal Information, including policies and practices with respect to the use of service providers outside Canada."

[268] 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.

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

Christine Sereda
Senior Information and Privacy Manager

# Appendix A: Babylon's Privacy Policy

## Babylon by TELUS Health Privacy Policy

At Babylon our mission is to put an accessible and affordable health service in the hands of every person on earth. We are passionate about high-quality and convenient healthcare. We are also passionate about privacy. We strive to be market leaders when it comes to healthcare and privacy, and always to comply with applicable privacy laws.

This policy explains how we collect, use, disclose and otherwise process your personal data when you use our healthcare services and products in Canada, or visit or use the App or any of our websites that link to this policy (collectively, our "App").

We want to help you understand how we work with your data, so that you can make informed choices and be in control of your information. We invite you to spend a few moments understanding this policy. We may update this policy from time to time and we will notify you when we do so.

This policy covers:

1. Who we are;
2. What personal data we hold and how we get it;
3. What we use your personal data for;
4. Sharing your personal data;
5. Retention;
6. Data security and transfers; and
7. Your rights.

If you have any questions about how we process your information, please don't hesitate to get in touch by contacting our Privacy Officer at privacyofficer@babylonhealth.com

## Who we are

Your relationship is with Babylon Health Canada Limited When this policy talks about 'Babylon', 'us', 'we' or 'our', it means Babylon Health Canada Limited.

What personal data we hold and how we get it

We use the following categories of personal data:

### Personal details

When you register with us, you complete forms and provide us with basic information about yourself, such as your name, date of birth, physical address and email address. You will also

provide us with a copy of identification documentation for ID checks to be carried out on our behalf by one of our service providers, and health card number/provincial health insurance number for the purposes of us billing the public health system. You are responsible for the accuracy of the information that you provide to us.

## Health and medical information

The main type of information we hold about you is health and medical information: information about your health, symptoms, treatments, test results, consultations and sessions, medications and procedures. This includes details of your consultations with our doctors, and interactions with our digital services, including interactions with our chatbot, symptom checker, 'Ask a doctor', Healthcheck, Digital Twin services, health monitoring, or other health and condition management services. Your interactions with our digital services may be shared with our doctors in order to provide you with a better experience and for the purposes of providing you health care.

We get some of this information directly from you, when you register with us and when you use our healthcare services. Any correspondence we receive from you is uploaded electronically to your Babylon medical record. We may also get this information from third parties, such as laboratories or other healthcare professionals.

We retain recordings of our consultations and interactions with you. This can include your use of our digital tools, such as chatbot, Healthcheck and monitoring services, video and audio recordings or audio-only recordings. This is in order to provide you with an easy way to check your consultations where you wish to, so that we can ensure high quality care is provided to you, and, with your consent, to allow us to learn from them to improve our services. To monitor our service quality, we may retain records of when you contact our support teams via email or phone. Recordings are held securely in accordance with our retention policy. You can access recordings of your consultations or interactions with us (depending on the format) for a limited time through the App or from us.

We may also hold information about you and your health from other apps, devices and services where you have given your consent to that data being shared with us. Examples include where you decide to share information collected from a smart watch or similar device with our App.

## Financial information

If you make any payments on the App, your credit/debit card details are processed directly by a third party processor that will store all payment information and transaction details. We will only retain details of transactions on secure servers and we will not retain your credit or debit card information.

## Technical information and analytics

When you use our App or visit our website, we may automatically collect the following information where this is permitted by your device or browser settings:

(a) technical information, including the address used to connect your mobile phone or other device to the Internet, your login information, system and operating system platform type and version, device model, browser or app version, time zone setting, language and location preferences, wireless carrier and your location (based on IP address); and

(b) information about your visit (such as when you first used the App and when you last used it, and the total number of sessions you have had on that App), including products and services you viewed or used, App response times and updates, interaction information (such as button presses or the times and frequency of your interactions with the communications we deliver to you in the App or otherwise) and any phone number used to call our customer service number.

We work with partners who provide us with analytics and advertising services (for our services only and not for third party advertising). This includes helping us understand how users interact with our services, providing our advertisements on the internet, and measuring performance of our services and our adverts. Cookies and similar technologies may be used to collect this information, such as your interactions with our services. You can change your device settings to block cookies, or to notify you before a cookie is set. If you block cookies, you may not be able to use all the features of our App. You can prevent the setting of cookies by adjusting the settings on your browser or your mobile phone.

## Information obtained from third party services

You may choose to connect your existing accounts with other providers (such as a social media provider), for example, when signing up to make it easier to create an account with us. If you choose to do this, we will receive limited information about you from that provider, such as your email address and name. Provided we are acting in accordance with data protection laws, we may also use information from other sources, such as specialist companies that supply information, online media channels, our commercial partners and public registers. This information can for example, help us to improve and measure the effectiveness of our services.

# What we use your personal data for

The purposes for which we use your personal data and the grounds on which we do so are set out below. We generally use personal data with your consent, except where the use of personal data without consent is permitted by law.

## Providing you a service

- We obtain and use your personal details and financial details in order to establish and deliver our contract with you and (if applicable) charge you correctly.

- 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. It may also include sharing information with other healthcare professionals as necessary for the provision of care to you, such as your GP, specialist referral services, therapists, pharmacists, hospitals, accident and emergency services, pathology service providers, and diagnosis centres chosen by you for the purpose of imaging request forms. It may also include Babylon physicians and their designates accessing your medical and / or prescription history contained within provincial databases (including but not limited to, PharmaNet, NetCare, Drug Profile Viewer) for the purpose of providing care or for the purpose of monitoring medication use.

## Making healthcare accessible

- Where you have provided your explicit consent, we will use your medical information (always having removed personal identifiers, such as your name, address and contact details) to improve our healthcare products and services, and our artificial intelligence system, so that we can deliver better healthcare to you and other Babylon users. This medical information (with your personal identifiers removed in the way described above) may include your medical record (both records received and created by us), transcripts and recordings of your consultations, and your interactions with our artificial intelligence services, such as our symptom checker and other digital tools. This does not involve making any decisions which would have a significant effect on you – it is only about improving our products, services and software so that we can deliver a better experience to you and other Babylon users, and help achieve our aim of making healthcare affordable and accessible to everyone. Strict confidentiality and data security provisions apply at all times. This consent relates to information that can identify you.
- 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.

## Keeping you up to date

- We use your email address, phone number and/or details to contact you or present you with occasional updates and marketing messages where you have not opted out, based on our legitimate interest in marketing our services to you and subject to your right to opt out at any time.

As part of providing you with high quality preventative and occupational health care services, we may contact you by SMS, email and/or other means to offer you helpful information or invite you to make appointments, for example for free healthcare screening programmes (such as cervical cancer screening).

## Other uses

- Based on our legitimate interest in managing and planning our business, we may analyse data about your use of our products and services to, for example, troubleshoot bugs within the App or our website, forecast demand of service and to understand other trends in use, including which features users use the most and find most helpful, and what features users require from us. This does not involve making any decisions about you that would have a significant legal effect on you – it is only about improving our App so that we can deliver better services to you. Strict confidentiality and data security provisions will apply at all times.
- Where necessary, we may need to share personal and financial details for the purposes of fraud prevention and detection.
- We also store your medical information, such as notes from consultations, recordings of our consultations with you as well as your interactions with our digital services including interactions with our chatbot (including symptom checker and 'Ask a doctor' and, Healthcheck and Digital Twin services), health monitoring, or other health and condition management services, for safety, regulatory, and compliance purposes. For example, we may need to review your information and, where necessary, make disclosures in compliance with lawful requests by regulatory bodies or as otherwise required by law or regulation.
- Where necessary for safety, regulatory and/or compliance purposes, we may audit consultations and your other interactions with our services. Strict confidentiality and data security provisions will apply at all times to any such audit and access.

# Sharing your personal data with others

We have partnered with TELUS Health to provide certain services on our behalf, including technical and customer support and communications. Your personal data will be shared with TELUS Health as necessary to allow TELUS Health to provide these services to you and to us. With your consent, we will also share your personal data, such as name and contact details (but not medical or health data) with TELUS Health so that TELUS Health can tell you about their products or services that might be of interest to you. We also share with TELUS Health de-identified data that is no longer capable of identifying you, as well as aggregated data that does not personally identify you, but which shows general trends, for example, the number of users of our service. If you are a user of the Babylon by TELUS Health Enterprise App provided by your employer, we and / or TELUS Health may share this de-identified, aggregated data with third parties, such as your employer.

- We may share your personal data with members of our corporate group to help us deliver our services to you.

- We share personal data (with identifiers removed) with members of our corporate group to help us develop, improve and maintain our software and artificial intelligence system (where you have explicitly consented to this use of your data).

- We may share your personal data with companies we have hired to provide services on our behalf, such as data hosting and processing, technical support, billing and payment processing, marketing and communications. These service providers are bound by strict confidentiality and data security provisions, and they can only use your data in the ways specified by us.

- Where you access our services through public or private health insurance, and where you have given your consent, we will need to let your insurance company know your name, email address, policy number, location (based on IP address), demographic information, that you had an appointment with us, the date of the appointment, details of your diagnosis, prescription, pharmacy location, whether or not you had a referral made and other similar information about your appointment with us.

## Information sharing with other healthcare providers

- We will, where necessary for your treatment or care, share your information with your other health and social care providers. For example, your GP, specialist referral services, therapists, pharmacists, hospitals, accident and emergency services, pathology service providers, diagnosis centers chosen by you for the purpose of imaging requests, and other health and care bodies. This may include sharing information with such services for safeguarding purposes in accordance with our legal or professional obligations.

- We may preserve or disclose information about you to comply with a law, regulation, legal process, or governmental request; to assert legal rights or defend against legal claims; or to prevent, detect, or investigate illegal activity, fraud, abuse, violations of our terms, or threats to the security of our services or the physical safety of any person.

- Our sharing of personal data with TELUS Health will always be in accordance with data protection laws and subject to strict safeguards.

Except as described above, we will never share your personal information with any other party without your consent.

# Retention

We retain your personal data and medical records for as long as necessary to provide the services you have requested and otherwise in accordance with legal, regulatory and self-regulatory requirements.

# Data storage, security and transfers

We do not store your personal health data on your mobile device. We store all your personal health data - including your primary care information, medication information and diagnostic information, on secure servers.

Where you have chosen a password that enables you to access certain parts of our App, you are responsible for keeping this password confidential. We ask you not to share the password with anyone.

We do not store any credit or debit card information. Payments are processed via a third-party payment provider that is fully compliant with Level 1 Payment Card Industry (PCI) data security standards. Any payment transactions are encrypted using SSL technology.

We encrypt data transmitted to and from the App. Once we have received your information, we will use strict procedures and security features to try to prevent unauthorised access.

We will take all steps reasonably necessary to ensure that your data is treated securely and in accordance with this privacy policy.

Your data may be processed stored or accessed by Babylon or our service providers from inside or outside of Canada, including in the European Union. In either case, personal data will be protected in accordance with data protection law and subject to strict safeguards. For example, when we do transfer personal data outside of Canada, we strive to minimize the amount of personal data that we transfer. Notwithstanding these safeguards, while outside of Canada, personal data may be accessible by foreign government agencies under applicable law.

## Your rights

As indicated above, whenever we rely on your consent to process your personal data, you have the right to withdraw your consent at any time by accessing the privacy settings in the App.

You may also have the right to:

- Request access to the personal data we hold about you. Recordings of your appointments with us and other medical notes can be accessed via the App. For other information, you can make a request by email;
- Ask us to rectify or erase information we hold about you, subject to limitations relating to our obligation to store medical records for prescribed periods of time;
- Ask us to restrict our processing of your personal data or object to our processing; and
- Ask for your data to be provided on a portable basis.

## Contact us

For any questions or concerns, or if you'd like information about how to lodge a complaint with us or an applicable privacy commissioner's office, you can contact us by sending an email to privacyofficer@babylonhealth.com.