Office of the Information and
Privacy Commissioner of Alberta

ABTraceTogether
Privacy Impact Assessment Review Report

July 2020

Alberta Health and Alberta Health Services

File 015714

Commissioner's Message

My office has completed an independent review of the privacy impact assessment (PIA) submitted by Alberta Health (AH), and endorsed by Alberta Health Services (AHS), for the ABTraceTogether contact-tracing app, and have accepted it, with recommendations.

Alberta's *Health Information Act* (HIA) requires that custodians prepare a PIA and submit it to my office for review and comment, before implementing a new practice or information system that involves the collection, use or disclosure of individually identifying health information.

A PIA is a process of analysis that requires custodians to consider privacy risks and mitigation measures to comply with HIA. Completing a PIA ensures that health care bodies and professionals turn their minds to privacy management at the outset of a new project.

When my office "accepts" a PIA, it is an acknowledgement that a custodian has made reasonable arrangements for the privacy and security of health or personal information. Acceptance is not a waiver or relaxation from any requirement of the relevant legislation once a practice or system is implemented.

Given the global attention currently focused on contact-tracing apps during the COVID-19 pandemic, I prioritized my office's review of ABTraceTogether. While I am not in a position to endorse a particular technology solution, I want to highlight certain features of the app that we paid particular attention to in our review:

- I appreciate that AH committed to a clear purpose for ABTraceTogether as a supplement to already established contact-tracing processes for addressing the COVID-19 pandemic. A technological approach alone is not a panacea. Combining technology with human oversight and public health expertise is a positive aspect of ABTraceTogether, and in my view reduces the risk for false-positive encounters.

- From our review of similar technologies implemented around the world, ABTraceTogether collects among the least amount of information at the time of registration. However, we noted during our review that there is a risk of over collection or disclosure regarding the Bluetooth contact logs ("handshakes").

- As noted in this report, consent is not an authority to collect health or personal information under HIA or the FOIP Act. Nonetheless, in order to enhance individual control of health and personal information, the ABTraceTogether app is voluntary. Individuals choose to download or register for the app to record Bluetooth encounter logs and choose to provide their encounter log to public health officials. These features support the privacy principle that individuals are able to control how their health or personal information is collected, used and disclosed.

- In previous public comments about the app, I raised a concern that information collected for ABTraceTogether, and disclosed to public health officials for contact-tracing purposes, could subsequently be used or disclosed for secondary purposes. For example, I questioned whether ABTraceTogether information may be used for law enforcement purposes, such as

quarantine enforcement. AH was responsive to this concern and, in addition to other project specific acceptable use policies, developed a policy that prohibits the use of information for quarantine enforcement.

- Given AH's focus on deploying the app, plans for decommissioning ABTraceTogether were not included as part of the initial PIA. During the review process, we received confirmation of AH's plan to decommission the app, and are generally satisfied as outlined in the report. We have asked to be involved when the time comes to dismantle the app, and have recommended AH report its decommissioning plans publicly.

Despite the above, I have ongoing concerns related to the functionality of ABTraceTogether, particularly on Apple devices. We recognize the challenges AH has faced in this regard, since the safeguards required to effectively run the app are out of its control. Nonetheless, given the need to run ABTraceTogether in the foreground on Apple devices, there is a security risk (e.g. when running the app, the device is unlocked, which increases risk in case of theft).

AH and AHS have a legal responsibility to safeguard personal and health information in their custody or control; however, my office does not regulate the actions of individuals who choose to download the app. AH has taken steps to provide information to individuals about functioning of the app. We have recommended that AH make information about potential privacy risks public, and update this information as necessary.

However, for employees in the public, health and private sectors who are issued devices by their employer or use their own devices for work purposes, the risk mitigation AH has put in place (i.e. providing information about risk) is not sufficient. The risks represent a potential contravention of Alberta's privacy laws by regulated entities for failure to safeguard if they were to allow or encourage employees or affiliates to run the app on enterprise-issued devices that store or make other health or personal information accessible (e.g. email or cloud service portals).

Given the above, it is unfortunate that there is currently no technical solution being made available to AH to address issues associated with running the app on Apple devices. We have asked AH to update us on progress towards resolving this problem, and to provide a PIA amendment if a solution is implemented.

AH has done an excellent job being mindful of privacy and security in the deployment of ABTraceTogether. The app's clear purpose, guided by principles of consent and individual control, is commendable. I want to thank the team at AH responsible for the PIA for their cooperation during this review. Their consultative approach, responsiveness, and transparency throughout the process has been greatly appreciated, and we look forward to hearing how ABTraceTogether progresses as we all work together to address the COVID-19 pandemic.

Jill Clayton
Information and Privacy Commissioner

Table of Contents

Background

[1] On Tuesday, April 7, 2020, Alberta Health (AH) informed the Office of the Information and Privacy Commissioner (OIPC) of its plan to implement a contact-tracing mobile application (the app or ABTraceTogether).

[2] AH described the app as a tool "to enable improved contact-tracing to inform the pandemic response activities by addressing limitations to the current process". It noted that "reliance upon individual's [sic] memories can be a challenge" and "many [physical] locations do not have a means of contacting those who were there". AH said that evidence from other jurisdictions "demonstrates the potential of such technology", and specifically highlighted the Singapore model, and its TraceTogether app, in an appendix.

[3] AH described its goals for the contact tracing app as follows:

- To interrupt ongoing transmission and reduce the spread of an infection.
- To alert contacts of the possibility of infection.
- To offer diagnosis and treatment to already infected individuals.
- To learn about the epidemiology (who, when, where and patterns) of an infectious disease.

[4] During its presentation to the OIPC, AH committed to:

- A "voluntary approach that is opt-in"
- "Clear communication around App use and information handling"
- "Limited collection of information"
- "Decentralized storage" of Bluetooth encounter logs
- Disclosing information to AHS "if and when contact tracing is required"
- Completing a privacy impact assessment (PIA)

[5] On Thursday, April 23, AH's Chief Medical Officer of Health (CMOH) announced publicly that Alberta's contact-tracing app was "in the final testing phase". Later the same day, the Information and Privacy Commissioner of Alberta (the Commissioner) publicly issued a statement saying her office had received a high-level overview of the program and that she anticipated reviewing a PIA on the app.

[6] On Monday, April 27, the OIPC received AH's PIA for ABTraceTogether.

[7] On Tuesday, April 28, the Commissioner assigned us to review the PIA. We had an initial call with AH on April 29 to identify key issues.

[8] AH launched ABTraceTogether on May 1, 2020. The app became available in the Google Play Store and Apple App Store, and was announced by the CMOH. The Government of Alberta (GoA) issued a news release, and published several webpages explaining how the app works and privacy protections in place.

[9] On that same day, May 1, we sent an initial set of questions to AH for response.

Jurisdiction

[10] Alberta's *Health Information Act* (HIA) provides health custodians, as defined by the Act, with a framework for collecting, using and disclosing health information.

[11] Section 64 requires custodians to prepare and submit PIAs to the OIPC for review and comment. Section 64 of HIA reads:

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

[12] AH is a custodian pursuant to section 1(1)(f) of HIA. As a result, it must submit a PIA for any new administrative practice or system relating to the collection, use and disclosure of individually identifying health information. Per section 64, AH is required to submit a PIA for ABTraceTogether.

[13] Alberta Health Services (AHS) is responsible "to analyze the app data and to notify individuals who may have encountered someone who has contracted COVID-19 and provide following advice [sic]". AHS is also a custodian as defined in HIA (section 1(1)(f)). As a result, it also must submit a PIA for ABTraceTogether.

[14] Alberta's *Freedom of Information and Protection of Privacy Act* (FOIP Act) provides public bodies, as defined by the Act, with a framework for collecting, using and disclosing personal information.

[15] AH is "a department, branch or office of the Government of Alberta", and is a "public body" as defined in section 1(p)(i) of the FOIP Act.

[16] AHS is also a "public body" as defined in section 1(p)(vii) of the FOIP Act, which states a "local public body" is a public body; a "local public body" includes a "health care body" under section 1(p)(j)(ii); and "health care body" includes a "regional health authority" under section 1(g)(ii). As a result, the FOIP Act applies to both AH and AHS' collection, use and disclosure of personal information.

Methodology

[17] We took the following steps during the course of our review:

- Reviewed a presentation provided by AH to the OIPC
- Reviewed the PIA submitted by AH and endorsed by AHS, which included:
  - ABTraceTogether: COVID-19 Contact Tracing Application PIA
  - Appendix A: Alberta Contact Tracing FAQ
  - Appendix B: ABTraceTogether Privacy Statement
  - Appendix C: IM Policy 029 ABTraceTogether
  - Appendix D: Acceptable Use Policy Statement Data Analytics
  - Appendix E: Acceptable Use Policy Statement – ABTraceTogether Case and Contact Tracing Portal Final
- Downloaded the app from the Google Play Store and Apple App Store and reviewed online information made available to users
- Sent written questions to AH (on May 1, May 25, June 18 and June 22), reviewed the responses (received May 7, May 19, May 28, June 23, June 30 and July 7), and sought additional clarification where required (a number of discussions took place throughout May, June and July)
- Reviewed information about contractual agreements between AH and third party service providers
- Requested and reviewed additional policy documents to enhance understanding of safeguards established by AH, including the ABTraceTogether quarantine enforcement information management policy
- Reviewed white papers and technical documentation on contact-tracing application frameworks, including BlueTrace,[1] OpenTrace,[2] and Apple[3] and Google's[4] exposure notification framework[5]
- Reviewed app details in the Google Play Store and Apple App Store, the privacy statement that is presented to the public when downloading the mobile app, and the frequently asked questions on the GoA's website

[18] AH's PIA submission followed the format of the OIPC's "Privacy Impact Assessment Requirements" guide.[6] For the most part, this report follows the same format, while also addressing some additional issues specific to the app.

---

[1] The Government Technology Agency of Singapore's "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders" white paper by Bay, et al is available from bluetooth.io.
[2] The "OpenTrace"website is available from github.com.
[3] Google and Apple's "Privacy-Preserving Contact Tracing" webpage provides "draft documentation for an Exposure Notification system" and is available from www.apple.com.
[4] Google and Apple's "Exposure Notifications: Using technology to help public health authorities fight COVID-19" provides an overview of their exposure notification system, and is available from www.google.com.
[5] Apple's "ExposureNotification" framework is available from developer.apple.com.
[6] The OIPC's "Privacy Impact Assessment Requirements" guide is available from www.oipc.ab.ca.

Project Summary

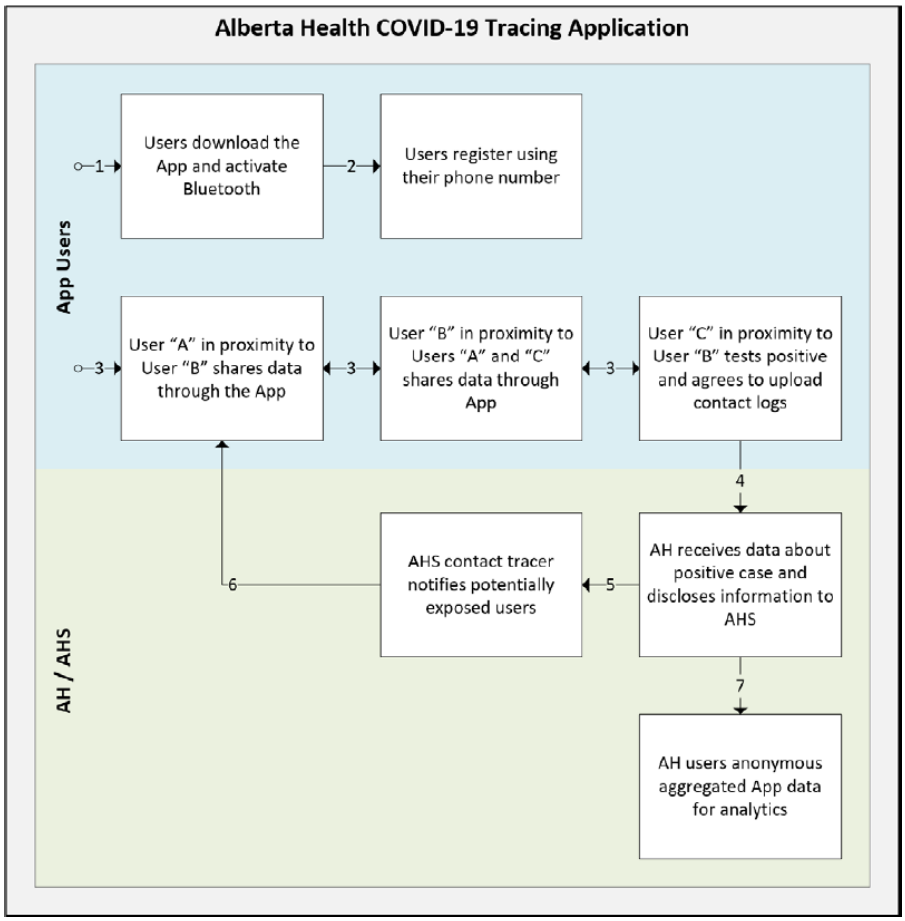
[19] AH's PIA says that "contact-tracing applications have become a powerful strategy in efforts to manage and limit the spread of COVID-19" leading to the development of ABTraceTogether with "both the information needs of Alberta's public health response and the privacy of Albertan's [sic] in mind." The PIA also says "the implementation of the App is part of a wider public health effort to quickly identify potential new flashpoints for COVID-19 transmission."

[20] The app "is based on the reference implementation application OpenTrace" and is available for download in the Google Play Store and Apple App Store.

[21] The PIA submitted by AH describes the app and various features, the ABTraceTogether portal and analytics environment, and identifies the following vendors:

- Deloitte (developed the app)
- IBM (hosts the servers)
- Twilio (provides SMS authentication services)

[22] The PIA includes the following information flow diagram which provides a high-level description of how the app works:



[23] Initially, users download the app and then register by providing their mobile phone number to AH. AH then creates a user ID that links to the mobile number. This user ID and phone number pairing are stored centrally by AH in the ABTraceTogether portal.

[24] The app installed on a user's phone communicates with other phones on which it is installed and the phones exchange Bluetooth logs (or "handshakes"). The Bluetooth logs contain "non-identifying information", including anonymous temporary IDs, device type, signal strength, date and time, and are initially stored locally on each user's device (decentralized, not accessible by AH) in an encrypted format. AH explained that "[temporary] IDs are generated from a combination of user IDs, start and expiry data, and are encoded and then encrypted". AH confirmed that "no GPS or geo-location features will be used by the App."

[25] The app maintains a 21-day history of data collected on the user's smartphone and is removed from the user's smartphone via automated rolling deletion. Information uploaded to the server from a user's smartphone is also "deleted after 21 days via automated rolling deletion. Deletion of the application also results in the removal of the stored data from the user's smartphone".

[26] AH noted that, "Once a user has tested positive for COVID-19, the App will provide information to enable case tracing and direction on how the user can voluntarily upload their information to AH." More specifically, "The application will send/display a code via SMS that is verified by both a contact tracer from AH [sic], and the user. After consenting to upload their data, users will enter a one-time passcode [OTP] to upload their logs. These logs are sent to the server-side infrastructure and stored for processing". The logs are transmitted to AH in encrypted format, and are stored in a database in Montreal.

[27] Once data has been uploaded by the user "[t]he data is decrypted by AH" and provided to AHS contact tracers. The data provided includes "[p]hone number (and) Anonymized IDs of positive case and any of their contacts within the last 21 days". AHS contact tracers use this information to "notify individuals who have potentially been in contact with the positive case".

[28] The PIA says contact tracers also use existing processes including the Communicable Disease Outbreak Management (CDOM) system. AH described CDOM as "an integrated public health information system that supports and enhances the delivery of public health services in the areas of communicable disease and outbreak management. It is a tool that helps Alberta Health and Alberta Health Services (AHS) meet their obligations to monitor communicable diseases and outbreaks under the [*Public Health Act*]."

[29] A de-identified version of the logs is also uploaded to the ABTraceTogether analytics environment. AH explained that records "will be strictly limited to anonymized, aggregate data collected by the App. Collected phone numbers will not be included." However, hashed user IDs and the other information collected when the user uploads their logs are analyzed in this environment.

Project Privacy

Health and Personal Information

[30] "Health information" is defined in section 1(1)(k) of HIA to mean "diagnostic treatment and care information" (section 1(1)(i)) and/or "registration information" (section 1(1)(u)).

[31] Section 1(1)(i) of HIA defines "diagnostic, treatment and care information" as follows:

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

[32] "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...[emphasis added]

[33] "Personal information" is defined in section 1(n) of the FOIP Act to mean "recorded information about an identifiable individual".

[34] AH's PIA included the following table of data elements collected, used and disclosed through ABTraceTogether:

Data Element	Description	Purpose
Phone number	A number that is uniquely tied to a specific phone	Used to identify positive COVID-19 cases for contact by public health officials.
User ID	A unique number assigned to a user	Used to uniquely identify each user of the App.
Anonymized ID	An anonymized ID number that is periodically changed through the use of rotating identifiers, and is shared with other App users within Bluetooth range	Used to uniquely identify each smartphone using the App and facilitate contact tracing.
Timestamp	Identifies the time at which two or more smartphones connected through the App	Used to establish and uniquely identify the connection between smartphones using the App.
Bluetooth signal strength	A measure of the Bluetooth signal strength on a given device	Used to establish and uniquely identify the connection between smartphones using the App and provide contact tracers with an estimate of distance between users.
User's smartphone model	Identifies the model of smartphone being used	Used to establish and uniquely identify the connection between smartphones using the App.

[35] AH confirmed that the mobile number collected during registration is both personal information to which the FOIP Act applies, as well as health information to which HIA applies.

[36] Information in the Bluetooth encounter logs that are uploaded by a user voluntarily after a COVID-19 diagnosis and used to notify other users about potential exposures (user ID, anonymized ID, timestamp, Bluetooth signal strength, user's smartphone model) is health information (diagnostic treatment and care information, as well as registration information) to which HIA applies.

Finding

- We accept that data elements collected, used and disclosed through ABTraceTogether are both health information to which HIA applies, and personal information to which the FOIP Act applies.

Authority to Collect, Use and Disclose Health and Personal Information

[37] Alberta's HIA and FOIP Act set out the circumstances in which custodians and public bodies are legally authorized to collect, use and disclose health and personal information, respectively.

[38] AH's PIA submission includes the following "Legal Authority and Purpose Table" (legal authority table) that describes the legal authorities relied on by AH and AHS to collect, use and disclose health and personal information through ABTraceTogether:

Flow #	Description	Type of Information	Purpose	Legal Authority
1	Users download the App	•Software application	App is voluntarily downloaded by users to assist public health officials with contact tracing	N/A
2	User Registration	•Phone number	Phone numbers are used to identify and notify App users who may have been exposed to COVID-19	Collection of health information by AH: HIA, s. 20(b), 22(1), 27(1)(a), 27(2)(c) FOIP Act, s. 33
3	Users in proximity to each other share data via Bluetooth, including their Temporary ID. Data is automatically deleted after 21 days	•Temporary ID; timestamp; Bluetooth signal strength; user's smartphone model	The data is used to identify the unique connections between different App users	Peer to peer information sharing that does not involve a collection, use or disclosure by AH
4	Users who test positive for COVID-19 upload their data (including their phone number). The data is decrypted by AH	•Phone number •Temporary IDs of positive case and any of their contacts within the last 21 days	The data is used to notify individuals who have potentially been in contact with the positive case	Collection of health information by AH: HIA, s. 20, (b), 22(2)(a), 22(2)(d), (e.2), 27(1)(a), 27(2)(c)
5	AH discloses data about positive case to AHS	•Phone number •User IDs of positive case and any of their contacts within the last 21 days	The data is used to notify individuals who have potentially been in contact with the positive case	Disclosure of health information to AHS by AH: HIA, s. 35(1)(a), s. 27(1)(a) and s. 27(2)(c) Collection of health information by AHS: HIA, s. 20, (b), 22(2)(a), 22(2)(d), (e.2), 27(1)(a), 27(2)(c)
6	App users who have been in contact with a positive case are notified by AHS contact tracer	•User IDs; phone numbers of contacts of positive case	Used to contact App users who have been in contact with the positive case	Use of personal information by AHS; HIA, s. 27(1)(a), 27(2)(c)
7	Anonymous, aggregate data is used by AH for analytics	•Anonymous, aggregate data collected from App users who voluntarily share the data with AH.	Used to measure App use and to determine where the App may need to be updated or improved (see Analytics section of the PIA for specifics)	Use of non-identifying data by AH and AHS: HIA, s. 26

[39] In **Flow 1** of the diagram, users download the app from the Google Play Store or Apple App Store. There is no collection, use or disclosure of health or personal information by AH or AHS, and therefore no authority required under HIA or the FOIP Act.

[40] When an individual registers to use ABTraceTogether, however, the individual provides their phone number to AH. AH says it collects this information in order to "identify and notify App users who may have been exposed to COVID-19" (**Flow 2**).

[41] More specifically, AH says:

> The initial information flow is listed as falling under both the *Health Information Act* and the *Freedom of Information and Protection Act* – individuals whose phone number is subsequently used as part of contact tracing would fall under the *Health Information Act* while those users whose phone number is never involved in contact tracing, as they do not test positive nor do they come in contact with a user who is positive fall under the *Freedom of Information and Protection of Privacy Act*. All other information flows reference authorities under the *Health Information Act*.

[42] AH's PIA says in the legal authority table that, for individuals that have registered but not tested positive or come into contact with someone who has tested positive, AH collects phone numbers under the authority of section 33 of the FOIP Act.

[43] Section 33 of the FOIP Act says:

> **33** No personal information may be collected by or for a public body unless
>
> (a) the collection of that information is expressly authorized by an enactment of Alberta or Canada,
> (b) that information is collected for the purposes of law enforcements, or
> (c) that information relates directly to and is necessary for an operating program or activity of the public body.

[44] AH did not originally specify which provision under section 33 of the FOIP Act authorizes its collection of personal information in ABTraceTogether, but later cited section 33(c) as its authority for the collection of personal information. AH said:

> It may be best to think of the App not as a new program, but as a tool that facilitates an existing program and existing activities that are authorized by statute. ABTraceTogether is a tool that facilitates the activities of the Chief Medical Officer of Health and the Medical Officers of Health to break the chain of transmission and prevent the spread of COVID-19, as authorized by the Public Health Act. In addition, the aggregate, non-identifying information assists the Minister with making policy decisions in relation to the pandemic. Some of his specific decision-making authorities are set out in the Public Health Act. Other decisions related to the pandemic fall within his broad authority as the Minister of Health under the Government Organization Act.

[45] If an individual later tests positive for COVID-19, AH relies on section 20(b) (for a purpose authorized under section 27), section 27(1)(a) (to provide health services) and section 27(2)(c)(to carry out public health surveillance within Alberta) to collect the phone number.

[46] **Flow 3** of the legal authority table refers to the exchange of temporary IDs, timestamp information, Bluetooth signal strength and the user's smartphone model for purposes of identifying "the unique connections between different App users".

[47] These information exchanges do not involve the collection, use or disclosure of health or personal information by AH or AHS, and therefore no authority is required under HIA or the FOIP Act.

[48] If an ABTraceTogether user is later diagnosed with COVID-19, they can choose to upload their Bluetooth encounter logs through the ABTraceTogether portal (**Flow 4**). The data (AH says this includes phone number,[7] temporary IDs of the user and the user's contacts within that last 21 days) is decrypted by AH. This represents a collection of health information by AH under HIA, relying on the authority of section 20(b) (collection for a purpose authorized under section 27), section 27(1)(a) (to provide health services) and section 27(2)(c) (to carry out public health surveillance within Alberta).

[49] In **Flow 5** of the legal authority table, AH discloses information about positive cases to AHS so that AHS can notify individuals who have potentially been in contact with the user who tested positive. This represents a disclosure of health information by AH, and a collection and use of health information by AHS.

[50] Section 35(1)(a) of HIA authorizes a custodian to "disclose individually identifying diagnostic, treatment and care information without the consent of the individual who is the subject of the information… to another custodian [AHS] for any or all of the purposes listed in section 27(1) or (2)". AH relies on section 35(1)(a) of HIA, in conjunction with section 27(1)(a) (to provide health services) and section 27(2)(c) (public health surveillance) to authorize the disclosure of health information to AHS.

[51] Once the information has been uploaded, AHS contact tracing staff are able to access the information through the ABTraceTogether portal (mobile number, user ID and Bluetooth encounter log details). This is a collection of health information under HIA by AHS. The PIA indicates AHS relies on section 20(b) (collection for a purpose authorized under section 27), section 27(1)(a) (to provide health services) and section 27(2)(c) (public health surveillance) for authority to collect this information.

[52] In **Flow 6**, the legal authority table indicates that AHS uses the health information "to contact App users who have been in contact with the positive case". The PIA also says that this information will be used to "form the basis for public health responses, including the notification of potentially exposed individuals, recommendations for self-isolation, as well as direction and advice for testing and treatment." This is a use of health information, which AH says is authorized by HIA under section 27(1)(a) (to provide health services) and section 27(2)(c)(public health surveillance).

[7] The BlueTrace white paper only describes phone number collected at registration.

[53] Finally, **Flow 7** of the legal authority table indicates that both AH and AHS use "[a]nonymous, aggregate data" for "analytics", and specifically "to measure App use and to determine where the App may need to be updated or improved".

[54] AH notes that section 26 of HIA says that, "A custodian may use non-identifying health information for any purpose." To the extent the information has been de-identified (see discussion later in this report), section 26 authorizes the use of this information for analytics purposes.

Finding

- In our view, the PIA establishes that AH and AHS have legal authority to collect, use and disclose health and personal information in ABTraceTogether.

Authority for Indirect Collection

[55] Custodians have a duty to collect health information directly from the subject individual, unless otherwise authorized by HIA. Section 22 of HIA says, in part:

> **22(1)** A custodian must collect individually identifying health information directly from the individual who is the subject of the information unless subsection (2) applies.
>
> **(2)** A custodian may collect individually identifying health information from a person other than the individual who is the subject of the information in the following circumstances:
>
> > (a) where the individual who is the subject of the information authorizes collection of the information from someone else…
> > (d) where collection from the individual who is the subject of the information is not reasonably practicable…
> > (e.2) where the custodian is conducting data matching for a purpose authorized under section 27…

[56] The legal authority table identifies two situations – **Flows 4 and 5** – in which AH and AHS do not collect health information directly from the individual who is the subject of the information.

[57] When an individual has been diagnosed with COVID-19 and volunteers to upload their Bluetooth encounter logs, "AH will collect the anonymized IDs of other users and inform them a user whom they have been in contact with has tested positive" (**Flow 4**). The collection of encounter logs by AH is an indirect collection.

[58] In **Flow 5**, AH discloses information about positive cases to AHS so that AHS can notify individuals who have potentially been in contact with the user who tested positive. This represents a disclosure of health information by AH, and a collection and use of health information by AHS. The collection by AHS is an indirect collection.

[59] For the indirect collections by AH and AHS, the PIA identifies section 22(2)(a) (indirect collection authorized by the individual), section 22(2)(d) (collection from the individual is not reasonably practicable) and section 22(2)(e.2) (data matching for a purpose authorized under section 27).

[60] With respect to sections 22(2)(a) and 22(2)(d) of HIA, AH said that the application of these authorities "is inherent in the operation of the App in so far as it is based on the premise of peer to peer exchange of 'handshakes' which is referenced in the App Privacy Statement." We accept that AH has adequately described how sections 22(2)(a) and 22(2)(d) apply.

[61] In addition, AH said, "The reference to section 22(2)(e.2) of the HIA was in error".

Finding

- In our view, the PIA establishes that AH and AHS have legal authority to collect health information indirectly pursuant to section 22(2)(a) (indirect collection authorized by the individual) and section 22(2)(d) (direct collection not reasonably practicable).

Notice

[62] When custodians collect health information directly from an individual, section 22(3) of HIA requires that they notify individuals about the purpose of the collection, the specific legal authority for the collection, and the title, business address and business telephone number of a person who can answer questions about the collection.

[63] Similarly, when collecting personal information directly from an individual, section 34(2) of the FOIP Act requires public bodies to notify individuals of the purpose for which the information is collected, the specific legal authority for the collection, and the title, business address and business telephone number of a person who can answer questions about the collection.

[64] When an individual downloads ABTraceTogether, both the Google Play Store and Apple App Store provide a high-level description of the app to potential users. We downloaded the app from the Google Play Store and Apple App Store and note that the descriptions detail "key benefits" of the app, including to "[a]ugment our current contact tracing efforts to provide guidance and care to those who are or may be infected". Information about the functioning of the app is provided, as well as a listing of the personal information that is collected.

[65] We did note, however, that the Google Play Store information says, "If a user tests positive for COVID-19, they will be contacted by an Alberta Health Services Contact Tracer, and asked to voluntarily upload their data to Alberta Health Services so that anyone the user came into close contact with over the previous 14 days can be notified". The reference to "previous 14 days" is inconsistent with information AH

provided to us in the PIA, which says contacts are logged for 21 days. We recommend AH review the description of the app available from the Google Play Store and Apple App Store to ensure it accurately describes the app.

[66] As part of the downloading process, the individual sees a webpage with the heading "Collection of Your Information" (privacy notice). This page says:

> The information you provide will be collected by Alberta Health and Alberta Health Services for the purpose of conducting contact-tracing during the COVID-19 pandemic response to manage the public health emergency under the Public Health Act.
>
> This information is collected under sections 20(b), 22(2)(a) & 27(2)(c) of the Health Information Act (HIA) and sections 33(a)&(c) & 34(1)(a)(i) of the Freedom of Information and Protection of Privacy Act (FOIP). Non-identifying information will be collected by Alberta Health for the purpose of reporting total numbers of registered users. Contact information of individuals receiving a positive diagnosis of COVID-19 will be collected for the purpose of conducting contact-tracing.
>
> Information provided may be used by Alberta Health for health system management and planning, policy development and analysis of the public health emergency, under section 27(2)(a)(b) and (d) of the HIA. Contact information will not be used for this purpose; only your random anonymized User ID and other de-identified data will be used.
>
> AB TraceTogether enables you to exchange non-identifying information with other users via Bluetooth; other users will not have access to any of your individually identifying information. If you receive a positive diagnosis for COVID-19, Alberta Health or Alberta Health Services will send you a code to enter into the Application. Your information will then be accessed and potentially disclosed by Alberta Health and Alberta Health Services to one another, for the purpose of facilitating contact-tracing during the COVID-19 pandemic, in accordance with the Public Health Act, section 27(1)(a) & 27(2)(c) & 35(1)(a) of the HIA, and section 39(1)(a) & 40(1)(c) of the FOIP. For more information please see the Privacy Statement.
>
> If you have questions about the collection of your information, please contact Alberta Health's HIA Help Desk, 21st Floor, ATB Place North, 10025 Jasper Avenue NW Edmonton AB, T5J 1S9, by phone at 780-427-8089 or email at HiaHelpDesk@gov.ab.ca

[67] At the end of the privacy notice page, there are buttons the user can click to "View Privacy Policy Online"[8] and "View FAQ". These resources provide more details about the app and how information is collected and used by AH and AHS, and answer common user questions. The privacy policy and FAQ are available from the GoA's website.[9]

[68] We reviewed these materials. The FAQ provides a general overview about the app and its purpose. It provides information and instructions for "Using the ABTraceTogether App" on Android and iOS devices, as well as information for disabling the app and deleting it. The FAQ also includes a section on "Privacy", which confirms that the app

---

[8] Clicking this link takes the user to a webpage with a section titled "Privacy Statement", as referred to in the privacy notice.

[9] The webpage for the ABTraceTogether Privacy Policy is available at www.alberta.ca/ab-trace-together-privacy.aspx. The FAQ is available at www.alberta.ca/ab-trace-together-faq.aspx.

does not collect location information. Information about the use of "anonymized" and "de-identified" data for analytics purposes is also provided.

[69] The privacy policy (or privacy statement) provides general information about the app, and explains the legal authorities for collecting, using and disclosing personal information. This information mirrors information included in the privacy notice. The privacy policy also includes information about withdrawing consent, record retention, data analytics, safeguards, limiting collection, and accessing and correcting information.

[70] In our view, the privacy notice appears to meet the requirements set out in section 22(3) of HIA and section 34(2) of the FOIP Act. The privacy notice:

- Identifies the purposes for which the health and personal information is collected ("conducting contact-tracing during the COVID-19 pandemic", "for health system management and planning, policy development and analysis of the public health emergency")
- Identifies various legal authorities for collection, use and disclosure ("sections 20(b), 22(2)(a) & 27(2)(c) of the *Health Information Act* (HIA) and sections 33(a)&(c) & 34(1)(a)(i) of the *Freedom of Information and Protection of Privacy Act* (FOIP)", "section 27(2)(a)(b) and (d) of the HIA", and "in accordance with the *Public Health Act,* section 27(1)(a) & 27(2)(c) & 35(1)(a) of the HIA, and section 39(1)(a) & 40(1)(c) of the FOIP")
- Includes contact information for individuals who may have questions about the collection of their information

[71] When comparing the privacy notice and the PIA's legal authority table, however, we noted a number of inconsistencies. For example:

- The privacy notice cites section 27(2)(a) (planning and resource allocation), section 27(2)(b) (health system management), section 27(2)(c) (public health surveillance) and section 27(2)(d) (health policy development) of HIA as authorities for collecting health information.
    - With respect to section 27(2), the legal authority table included in the PIA only references section 27(2)(c).
- The privacy notice cites section 33(a) (collection expressly authorized by an enactment of Alberta or Canada) and section 33(c) (collection relates directly to and is necessary for an operating program) of the FOIP Act as authorities for collecting personal information.
    - The legal authority table cites "s. 33"; however, AH has since clarified that it relies on section 33(c), not section 33(a).

- The privacy notice says, "Your information will then be accessed and potentially disclosed by Alberta Health and Alberta Health Services to one another, for the purpose of facilitating contact-tracing during the COVID-19 pandemic…".
    - The legal authority table only describes a disclosure of health information to AHS, not any disclosure "by Alberta Health and Alberta Health Services to one another". We asked AH to clarify; however, its response did not describe any disclosures from AHS to AH.
- The privacy notice also says such accesses and disclosures are "in accordance with the *Public Health Act*, section 27(1)(a) & 27(2)(c) & 35(1)(a) of the HIA, and section 39(1)(a) & 40(1)(c) of the FOIP".
    - The legal authority table does not mention section 39(1)(a) of the FOIP Act (use of information for the purpose for which the information was collected or compiled or a use consistent with that purpose) or section 40(1)(c) of the FOIP Act (disclosure of personal information in accordance with Part 1 of the FOIP Act). When asked to clarify this discrepancy, AH said that section 39(1)(a) "applies as the information collected will be used for the purposes set out in the Privacy Statement", and that section 40(1)(c) "applies as the information collected may be disclosed by Alberta Health to Alberta Health Services for the purposes set out in the Privacy Statement." We further note this appears inconsistent with other responses AH provided with regard to when HIA or the FOIP Act applies to the use or disclosure of a phone number.
- The privacy notice cites section 34(1)(a)(i) of the FOIP Act for authority to collect personal information indirectly.
    - The legal authority table does not reference section 34(1)(a)(i) of the FOIP Act. With respect to this discrepancy, AH said, "Alberta Health plans to update and clarify the privacy statement with a future release and will remove the reference to this authority."
- The privacy notice does not reference sections from HIA that authorize the use of non-identifying health information for any purpose. The privacy notice does, however, describe how AH will use non-identifiable information.
    - The legal authority table references sections from HIA that authorize the use of non-identifying health information for any purpose (i.e. section 26 of HIA).
- The privacy notice does not reference the same sections from HIA that authorize indirect collection of health information. The notice includes section 22(2)(a) of HIA;

however, it does not reference sections 22(1), 22(2)(d) and 22(2)(e.2),[10] which are listed in the legal authority table.

[72] We also noticed some inconsistencies in the FAQ with respect to legal authorities. The FAQ says, with respect to analytics data, that, "Information provided may be used for health system management and planning, policy development and analysis of the public health emergency". While it clarifies that only "random anonymized User ID and other de-identified data" will be used in the analytics environment, this is nonetheless inconsistent with the legal authorities AH cited in the PIA's legal authority table.

[73] The privacy policy also includes information about AH and AHS' legal authority to collect, use and disclose health and personal information, and mirrors the information in the privacy notice, including the inconsistencies described above in the PIA's legal authority table.

[74] In addition to the above, we note that in response to questions, AH said the following in respect of the Bluetooth encounter logs (i.e. app-to-app interactions or "handshakes") that are disclosed by AH to AHS contact tracers:

> AB TraceTogether exchanges temporary IDs with other phones running AB TraceTogether. All of these "hand shake" interactions are logged on the phone. Exposure time and distance metrics are calculated [by contact tracer staff] based on Bluetooth signal strength at the time of the "hand shake".
>
> When an individual agrees to upload their set of encounter logs, all the "hand shakes" are uploaded to the contact tracing portal. These are aggregated up to identify where a risk for exposure may have occurred. Exposures lasting 15 minutes or more at a distance of 2 meters or closer are identified for the contact tracers to follow up on. The requirement for 15 minutes of exposure at a distance of two meters or closer is based off of the current clinical guidance available. Based on revised guidance this exposure requirement may change in the future. There is also discretion that can be exercised by the Contact Tracer based on their discussion with the individual who has tested positive to help determine who of the contacts may have exposure risk.
>
> To answer your question more directly, all of the "hand shakes" that occur are logged; however the contact tracer portal aggregates and filters those encounters that meet the exposure threshold…

[75] In our view, given information in public-facing documents, it may not be clear to users of the app that "all" of the "handshakes" that occur are logged. The app has generally been described publicly as recording encounters that are two metres or closer and a minimum of 15 minutes in duration.

Findings

- Information provided through the Google Play Store and Apple App Store refers to Bluetooth encounter logs that are retained for "14 days", which is inconsistent with

[10] AH has since clarified that the reference to HIA section 22(2)(e.2) was an error.

information AH provided in its PIA, and our understanding of how the app functions (i.e. contacts are logged for 21 days).
- There are a number of inconsistencies between information included in the privacy notice, FAQ and privacy policy with the information included in the PIA's legal authority table.
- In our view, it would not be clear to users of the app that "all" of the "handshakes" that occur are logged, given the app has generally been described publicly as recording encounters that are two meters or closer and a minimum of 15 minutes in duration.

Recommendations

- We recommend AH review the description of the app available from the Google Play Store and Apple App Store to ensure it accurately describes the app.
- We recommend that AH review and confirm its authority to collect, use and disclose health and personal information under HIA and the FOIP Act, as well as the purposes for which it collects, uses and discloses this information, and update the PIA, privacy notice, FAQ and privacy policy accordingly.
- We recommend that AH review public materials describing the app's functionality to ensure that it is clear that the app logs all "handshakes", and the purpose for doing so.

Consent

[76] As has been discussed previously, Alberta's HIA and FOIP Act set out the circumstances in which custodians and public bodies are legally authorized to collect, use and disclose health and personal information, respectively.

[77] We note that consent is not an authority to collect or use health information under HIA, and is not an authority to collect personal information under the FOIP Act. Instead, ABTraceTogether is a voluntary app that individuals choose to download. When an individual registers for the app, they voluntarily provide their phone number as part of the process. If an individual user later tests positive for COVID-19, the individual again has a choice about whether they will provide their encrypted Bluetooth encounter logs to AH, for subsequent disclosure to AHS for contact tracing purposes.

[78] As noted above, the PIA's legal authority table establishes that AH and AHS have legal authority to collect, use and disclose health and personal information through ABTraceTogether without relying on consent.

[79] Nonetheless, the privacy notice that individuals see when they register for ABTraceTogether includes a "consent statement" for the use and disclosure of health and personal information in some circumstances.

[80] AH explained its reasoning behind the consent:

> Alberta Health considered carefully the positioning of the App and its associated approach. Public buy-in and support is critical to its adoption and success. Alberta Health believes that the consent-based approach provides Albertans with both choice in the use of the App as well as how their information will be handled. The intent is that this decision will encourage buy-in and lead to greater adoption by Albertans, thereby helping to ensure the success of the initiative. Although consent is not a requirement, it was ultimately decided that alternative approaches which did not directly address individual consent and control over information were not consistent with the design philosophy of the App and the need to obtain broad public support for the initiative to be successful. Voluntary adoption of the app in combination with express consent is a more user centric approach than only voluntary adoption. Furthermore, consent can be revoked, which creates clear control for users to off-board and have their information removed.

[81] The consent statement reads as follows:

> By accepting the terms and conditions set out in this summary privacy notice, you:
>
> a. consent to the **use and potential disclosure** of your personal and health information by Alberta Health and Alberta Health Services **to one another** in accordance with section 39(1)(b) of FOIP, and section 34 of HIA, for the purposes described above; and
>
> b. acknowledge that you understand why the **disclosure** of this information may be necessary, and the risks and benefits of consenting or refusing to consent.
>
> This consent may be revoked at any time by emailing HiaHelpDesk@gov.ab.ca with the mobile number you registered in the Application. [emphasis added]

[82] Users are prompted to toggle to "agree to the privacy policy".

[83] Section 39(1)(b) of the FOIP Act (which is referenced in the consent statement) says, "A public body may use personal information only… if the individual the information is about has identified the information and consented, **in the prescribed manner**, to the use" [emphasis added].

[84] The "prescribed manner" is set out in section 7 of the Freedom of Information and Protection of Privacy Regulation (FOIP Regulation) which sets out the requirements for any consent obtained under section 39(1)(b). In particular, the consent "must specify to whom the personal information may be disclosed and how the personal information may be used" (section 7(2)(b)). In addition, section 7(5) of the FOIP Regulation sets out a number of requirements for a "valid" electronic consent.

[85] Similarly, section 34 of HIA authorizes disclosures of health information with consent, and sets requirements for electronic consent. Section 34 says:

> **34(1)** Subject to sections 35 to 40, a custodian may disclose individually identifying health information to a person other than the individual who is the subject of the information if the individual has consented to the disclosure.
>
> **(2)** A consent referred to in subsection (1) must be provided in writing or electronically and must include

(a) an authorization for the custodian to disclose the health information specified in the consent,
(b) the purpose for which the health information may be disclosed,
(c) the identity of the person to whom the health information may be disclosed,
(d) an acknowledgment that the individual providing the consent has been made aware of the reasons why the health information is needed and the risks and benefits to the individual of consenting or refusing to consent,
(e) the date the consent is effective and the date, if any, on which the consent expires, and
(f) a statement that the consent may be revoked at any time by the individual providing it…

[86] Section 6(2) of the Health Information Regulation (HIA Regulation) sets additional requirements for electronic consent. It says, "For the purposes of sections 34 and 59 of HIA, an electronic consent or a revocation of an electronic consent is valid only if the level of authentication is sufficient to identify the individual who is granting the consent or revoking the consent…".

[87] We reviewed the consent statement along with the privacy statement and other public-facing documents. In our view, the consent does not meet all of the requirements of section 34(2) of HIA. For example, while the consent statement includes an acknowledgement that the individual has been made aware of the "risks and benefits", we note the privacy notice and FAQ do not describe all privacy risks (e.g. see section below on "Functionality").

[88] Despite this, we have already said that AH and AHS have the legal authority to collect, use and disclose health and personal information through ABTraceTogether without relying on consent.

Findings

- AH and AHS have the legal authority to collect, use and disclose health and personal information through ABTraceTogether without relying on consent. AH has decided that a consent-based approach provides Albertans with more choice and control.
- In our view, the voluntary nature of the app and the consent-based approach by AH is consistent with the privacy principle that individuals are able to control how their personal information is collected, used and disclosed. The consent AH is using, however, does not meet the requirements of HIA or the FOIP Act, potentially causing confusion.

Recommendation

- We recommend AH review the wording of the consent against the requirements set out in both HIA and the FOIP Act to ensure the requirements are met and to avoid confusion.

Limited Collection, Use and Disclosure

[89] Sections 57 and 58 of HIA require custodians to collect, use and disclose health information with the highest degree of anonymity possible and to collect, use and disclose health information in a limited manner.

[90] Section 33(c) of the FOIP Act states, "No personal information may be collected by or for a public body unless… that information relates directly to and is necessary for an operating program or activity of the public body."

[91] As described by AH, ABTraceTogether collects only minimal information necessary to assist contact-tracing processes (i.e. user's phone number) during the registration process. Once running, the app exchanges rotating, anonymous IDs, timestamps, signal strength and the model of smartphone being used. The BlueTrace whitepaper refers to these exchanges as "handshakes". The analytics program collects only aggregate, de-identified information.

[92] Users who choose to register for the app may choose to provide their encrypted Bluetooth encounter logs (or "handshakes") to AH, for disclosure to AHS.

[93] We understand that capturing "handshakes" is directly related to and necessary for the app's purposes (i.e. for contact tracers to assess risk of exposure and notify potentially exposed individuals accordingly).

[94] However, it is not clear to us what the distance threshold is for capturing "handshakes". That is, AH appears to be saying that individual smartphones will collect encounter information for contacts that are greater than two metres; however, AHS did not provide information describing the actual distance threshold (i.e. five, 10 or 20 metres).[11]

[95] Further, we note that Bluetooth ranges can vary, resulting in the potential collection of "handshakes" beyond the exposure threshold of two meters.[12]

[96] AH describes how ABTraceTogether uses these handshake records to approximate distance based on "Received Signal Strength Indicator (RSSI) readings" and contact duration by "add(ing) up all exposures" to determine which encounters meet the thresholds to constitute a close contact. AH said:

> AB TraceTogether exchanges temporary IDs with other phones running AB TraceTogether. **All of these "hand shake" interactions** are logged on the phone. Exposure time and distance metrics are

[11] The Government Technology Agency of Singapore's "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders" white paper by Bay, et al discusses Bluetooth accuracy noting on p. 5 that, "Bluetooth has a range of 10 metres in indoor environments, but RSSI [Received Signal Strength Indication] follows inverse square law and drops off quickly with distance. However, calibration is necessary for maximal effectiveness as different devices transmit at different powers." The white paper is available from bluetooth.io.

[12] Bluetooth discusses range between Bluetooth devices on a webpage on "Understanding Bluetooth Range" that is available from www.bluetooth.com.

> calculated [by contact tracer staff] based on Bluetooth signal strength at the time of the "hand shake".
>
> The app applies the definition of close contact used in Alberta (approximately 2 metres) for contact tracers to determine whether a user has had probable exposure to COVID-19. The app uses Received Signal Strength Indicator (RSSI) readings to determine if app users have been within approximately 2 meters of each other. [emphasis added]

[97] AH added:

> The initial threshold of what constitutes a close contact was set at 15 minutes of exposure at 2 meters or less. This threshold was set based on established clinical guidance but may be adjusted over time, based on additional evidence...

[98] Therefore, it was our understanding that only "handshake" interactions that meet the clinical guidance threshold are logged. We asked AH about this issue, and AH indicated:

> The app does not discard "handshakes" that are at a further distance or time outside the current threshold. The information is collected and is necessary to add up all exposures and determine notification as well as to provide for adjustments based on new guidance or case specific factors.
>
> The "handshakes" are aggregated upon upload to the contract tracer portal. This aggregation takes the individual "handshakes" and adds up the exposure time and distance between two users. A single "hand shake" may not result in close contact; while a series of "handshakes" may hit the threshold for notification as a possible exposure.
>
> In some circumstances individuals who test positive may be determined to have different propensities to transmit the virus. By collecting all "handshakes" contact tracers are provided with discretion around determining who may be at risk for exposure and can potentially include individuals at a further distance with a shorter exposure time based on evidence or factors presenting to them as part of a particular case.

[99] While AH did not define a maximum range within which handshakes could be exchanged, AH provided the following explanation on the lack of technical safeguards to limit collection of encounter logs:

> [B]ased on the variability of the strength of signals across various devices and manufactures [sic] it would be technically problematic to attempt to set an on App filter; as it could filter out situations where a concern for exposure was warranted.

[100] AH's assertion that signal strength varies is consistent with the BlueTrace whitepaper, and our research into the Bluetooth protocol. Specifically, the Bluetooth protocol performance is based on numerous factors such as device manufacturer, "receiver sensitivity", "transmit power" and "path loss… attenuation [that] occurs naturally over distance and is impacted by the environment in which the signal is being transmitted. Obstacles between the transmitter and the receiver can deteriorate the signal."[13]

[13] Ibid.

[101] We acknowledge that technical safeguards for limiting collection based on signal strength (RSSI), as a proxy for approximate distance, may be a challenge for AH due to the difficulties in reliably equating RSSI values to distance. The matter is further complicated by the Bluetooth protocol, environmental impacts on its performance, and any limitations of the BlueTrace protocol itself.

[102] We note that AH provided a number of post-collection mitigation strategies to address the potential over collection, including:

> [W]hen the "handshakes" are uploaded, the contract tracer portal adds these up and does not display those below the threshold. While all "handshakes" are collected by the App and subsequently uploaded the contact tracing portal provides a control to limit the use of information; specifically that the identity of those who are below the exposure threshold for a close contact are not revealed to a contact tracer.

[103] The PIA indicates "analytics will also help AH determine how and to what extent the App needs to be updated or modified to ensure it remains as accurate and useful as possible", including "opportunities to tune the distance threshold" and "opportunities to tune the duration threshold", leaving open the possibility of adjusting the measures used by AH in determining exposure. It is unclear if such tuning would present an opportunity to limit collection in future iterations of the app.

[104] Further, we acknowledge that ABTraceTogether augments established contact-tracing processes, where the analysis of "handshakes" may reduce the risk for false-positive encounters, mitigating some risks resulting from using RSSI to approximate encounter distance. However, filtering encounter logs after the collection of handshakes may not meet the requirement in HIA to collect "only the amount of health information that is essential to enable the custodian… to carry out the intended purposes" (section 58). Therefore, in our view, the collection of all handshakes, not only those within two metres, may be an over collection (by AH) or disclosure (to AHS) of Bluetooth encounter logs.

Finding

- We acknowledge there are challenges to technically limiting the over collection of Bluetooth encounter logs or "handshakes" at distances greater than two metres, due to the nature of the technologies (i.e. Bluetooth, BlueTrace protocol) involved. Therefore, in our view, the collection of all handshakes, not only those within two metres, may not meet the requirement in HIA to collect (by AH) or disclose (to AHS) "only the amount of health information that is essential to enable the custodian… to carry out the intended purposes" (section 58).

Recommendation

- We recommend that AH work towards limiting collection of "handshakes" through any means available to them, to be transparent to the public regarding potential over collection, and to update the PIA, as necessary, if changes are introduced.

Data Matching

[105] Section 1(1)(g) of HIA defines data matching to mean "the creation of individually identifying health information by combining individually identifying or non-identifying health information or other information from 2 or more electronic databases, without the consent of the individuals who are the subjects of the information".

[106] The OIPC's "Privacy Impact Assessment Requirements" guide requires custodians to explain if health or personal information involved in a project will be linked, matched or otherwise combined with health information from other sources. If a custodian is data matching, the custodian must describe how it has mitigated privacy risks (e.g. making anonymized data identifiable).

[107] With respect to data matching, AH's PIA says:

> User IDs and line level data will be copied into Alberta Health's analytics environment and will persist for 18 months. **This data will be compiled with information from other systems but data matching as defined by the HIA will not be occurring as individual identifying health information will not be created.** [emphasis added]

[108] We understand from the PIA that contact tracers are using existing processes including the Communicable Disease Outbreak Management (CDOM) system. AH described CDOM as "an integrated public health information system that supports and enhances the delivery of public health services in the areas of communicable disease and outbreak management. It is a tool that helps Alberta Health and Alberta Health Services (AHS) meet their obligations to monitor communicable diseases and outbreaks under the [*Public Health Act*]." AH and AHS have submitted a PIA and a PIA amendment on CDOM.

[109] AH also said that when it receives Bluetooth encounter logs, "decrypted data will be cross-referenced with the [user] ID and phone number of other users" to enable contact tracing. As mentioned above in the section on "Authority for Indirect Collection", AH clarified that, "Although the contact-tracing process itself involves matching the data of users to determine potential exposures to COVID-19, the program does not perform data matching as defined in the HIA."

[110] AH confirmed that, "There is no connection or information flow between ABTraceTogether and the CDOM system. CDOM is only used as a case-management tool

for contract tracers, allowing them to work with positive cases and undertake appropriate follow up."

[111] Because ABTraceTogether is meant to support existing contact-tracing processes, we asked if health information from ABTraceTogether would be stored in any other system. AH said, "No information from ABTraceTogether is stored in a patient's medical record. However, if a user is flagged as having been exposed to COVID-19 and contact tracers are performing a follow up, the contact tracer may make a note indicating the user was exposed. In these instances the user's ID, phone number and other exposure details will not be copied or stored in the patient's medical record."

[112] We understand this to mean that AHS staff may document an exposure, learned from ABTraceTogether, in another medical record system. While AH has assured us that this is not data matching as defined by HIA, it has not provided us with enough information to adequately explain its position. We are unable to confirm whether this is or is not data matching. We recommend AH provide additional details to explain why it does not consider this data matching.

Finding

- It is not clear to us from information provided whether data matching is taking place, specifically in relation to CDOM and other medical record systems.

Recommendation

- We recommend that AH provide additional information to clarify its position. If data matching is taking place, AH is required (by Part 6, Division 2: Data Matching of HIA) to explain how risks are mitigated.

Project Privacy Risk Mitigation or Safeguards

[113] Section 60 of HIA requires custodians to take reasonable steps to protect the confidentiality of records under their custody and control.

[114] Section 38 of the FOIP Act requires that the head of a public body protect personal information "by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction."

[115] AH's PIA described the safeguards in place to prevent unauthorized collection, access, use or disclosure of health and personal information. Given the nature of ABTraceTogether, we focused our review on administrative and technical safeguards.

Administrative Safeguards

[116] Administrative safeguards typically include organizational and project specific policies and procedures, training, risk assessment tools (i.e. PIAs), and security in contracting.

Organizational Privacy Management

[117] When custodians submit PIAs to the Commissioner as required by section 64 of HIA, the OIPC's "Privacy Impact Assessment Requirements" guide mandates that they describe how privacy is generally managed within their organization. The PIA must include details on organizational privacy governance (roles and responsibilities), privacy policies and procedures, privacy training, how access and correction requests are handled, technical safeguards such as network privacy and security, monitoring and auditing procedures.

[118] Some custodians submit "Organization and Information Management PIAs" for this purpose, and then notify the OIPC if aspects of their privacy management program change (e.g. policies are updated).

[119] Organization and information management PIAs are typically submitted by larger custodians that may have several projects underway, such that project specific PIAs can be submitted separately and refer to a previously accepted organization and information management PIA.

[120] With respect to organizational privacy management and ABTraceTogether, AH referred us to the "Alberta Health Organizational PIA OIPC File # H4562" which was accepted by the OIPC in 2012.

[121] We note that AHS most recently submitted an updated organization and information management PIA to the OIPC in November 2019; however, that PIA has not yet been accepted.[14] The OIPC has asked for clarification on several aspects of that PIA.

[14] Because AHS does not have an up to date organization and information management PIA accepted by the OIPC, the OIPC is not currently accepting any project PIAs submitted by AHS.

Findings

- The OIPC has previously accepted AH's Organization Privacy Management PIA.
- AHS submitted an updated Organization Privacy Management PIA in November 2019 that has not yet been accepted.

Recommendation

- We recommend AHS address any outstanding issues with its Organization Privacy Management PIA.

Project Specific Policies and Procedures

[122] In addition to AH's general policies and procedures as described in its organization and information management PIA, AH provided us with the following project specific policies: [15]

- "IM Policy 029 AB Trace Together" (IM Policy)
- "Acceptable Use of AB TraceTogether Data for Analytics Policy Statement" (Analytics Acceptable Use Policy)
- "Acceptable Use of AB TraceTogether Contact Tracing Portal" (Contact Tracing Acceptable Use Policy)

[123] The IM Policy generally states that AH will "collect limited amounts of personal and health information". Individually identifying health or personal information may only be used "for the purpose of facilitating case and contact tracing related to the COVID-19 pandemic, and administering user registration and offboarding". The policy says that AH "may use aggregate data collected via the App for reporting the number of users". This information will be stored for 18 months, and "may be accessed by authorized affiliates to perform analytics for planning, health system management, policy development and analysis of the public health emergency". The policy prohibits use of health or personal information "for any purpose not authorized by this policy".

[124] The Analytics Acceptable Use Policy also says that AH and AHS "will use limited amounts of personal and health information obtained via AB TraceTogether". It also says "you have been approved to work with AB TraceTogether data for planning, health system management, policy development and public health surveillance purposes". The policy prohibits access and use of information collected via ABTraceTogether for any other purpose, and specifically says "you are only authorized to access and use information necessary for you to respond to your assigned files/workload". It also says, "All accesses

[15] AH also provided its FAQ document and privacy policy (or privacy statement). These are public documents, not internal. Discussion on these documents is included in the "Notice" section of this report.

to information by Alberta Health and Alberta Health Services affiliates will be logged and subject to auditing and reviews".

[125] The Contact Tracing Acceptable Use Policy similarly says AH and AHS "will use the least amount of personal and health information obtained via AB TraceTogether". It also says:

> You have been approved to work with AB TraceTogether data for contact tracing. You must only access and use information collected via AB TraceTogether during the public health emergency response for the purpose of facilitating contact tracing of individuals possibly exposed to COVID-19. No other use or disclosure is permitted.
>
> As an approved user, you are only authorized to access and use information necessary for you to respond to your assigned files, cases and/or workload. All accesses to information by users will be logged and subject to auditing and reviews.

[126] We generally accept that these project specific policies are reasonable for ABTraceTogether. However, with respect to the IM Policy and Analytics Acceptable Use Policy, we note the same concern we raised previously concerning the online FAQ document and privacy policy. The IM Policy says that analytics information "may be accessed by authorized affiliates to perform analytics for planning, health system management, policy development and analysis of the public health emergency". The Analytics Acceptable Use Policy says data will be used "for planning, health system management, policy development and public health surveillance purposes". These statements are inconsistent with one another, and with the PIA's legal authority table.

[127] Despite the above policies prohibiting unauthorized or secondary use of data, we advised AH of our concern that, once health and personal information has been collected by a custodian or public body, HIA and the FOIP Act will apply to that information. Both Acts authorize secondary uses and disclosures of information, including to law enforcement (e.g. section 37.3(1) of HIA and section 40(1)(q) of the FOIP Act).

[128] In response to this concern, AH said:

> AB TraceTogether is designed and functions to support the process of contact tracing; it is not designed to support quarantine enforcement. The App does not capture information that will be used to enforce a quarantine and further due to the lack of GPS information, what information the App does collect is not particularly effective or reliable for such a purpose. In addition, Alberta Health has explicitly made use of information for such a purpose out of scope for this project.

[129] During the course of our review, AH established a policy that information collected from ABTraceTogether will not be disclosed to law enforcement or other organizations for the purpose of enforcing quarantine. The policy is titled "IM Policy 030 Use of AB TraceTogether Not Authorized for Quarantine Enforcement", and says:

> Alberta Health and Alberta Health Services and their respective affiliates shall not use or disclose information collected via AB TraceTogether for quarantine enforcement measures; this includes disclosures to law enforcement for the purpose of enforcing quarantine requirements.

> Affiliates authorized to access information collected via AB TraceTogether must do so in accordance with the AB TraceTogether Analytics Portal Acceptable Use Policy and/or the AB TraceTogether Case and Contact Tracing Portal Acceptable Use Policy and for no other purpose.

[130] AH also noted that, in addition to the administrative control established by this policy, there is also a technical control to reduce risk as the information is only retained for a 21-day period before being automatically deleted.

Findings

- We generally accept that AH has developed reasonable project specific policies for ABTraceTogether.
- In our view, there is a risk that information collected through ABTraceTogether could be used for quarantine enforcement. In addition to other project specific acceptable use policies, AH developed a policy that prohibits the use of information for quarantine enforcement. "IM Policy 030 Use of AB TraceTogether Not Authorized for Quarantine Enforcement" policy is an acceptable risk mitigation measure.

Recommendation

- We recommend that AH review its policies, particularly concerning access to and use of data in the analytics environment, as well as the legal authorities cited in the PIA's legal authority table, to ensure consistency.

Risk Assessment (PIA Compliance)

[131] Preparing a privacy impact assessment and submitting it to the Commissioner for review is an important administrative safeguard to protect against risks to privacy. Section 64 of HIA requires custodians to prepare and submit PIAs. Section 64 of HIA reads:

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

[132] The FOIP Act does not require public bodies to submit PIAs to the OIPC for review.

[133] As previously noted, the OIPC received the ABTraceTogether PIA on Monday, April 27.

[134] AH launched ABTraceTogether on May 1, 2020.

[135] That same day, May 1, AHS sent a letter to the OIPC referencing the ABTraceTogether PIA submitted by AH. The letter stated:

> Alberta Health Services (AHS) involvement is to analyze the app data and to notify individuals who may have encountered someone who has contracted COVID-19 and provide following advice. The implementation of AB TraceTogether is part of a wider public health effort to quickly identify potential new flashpoints for COVID-19 transmission. AHS has reviewed the Alberta Health PIA and associated appendices and AHS endorses the submission of the PIA to the OIPC.

[136] When an initiative involves more than one custodian and the PIA describes how each custodian is participating and meeting the requirements of HIA, one custodian may submit the PIA and the others may submit letters of endorsement. The OIPC has established a practice whereby it will accept a PIA letter of endorsement that meets the requirements of section 64.

[137] With respect to any future changes to ABTraceTogether, AH said:

> Reviews of any projects, processes or systems that involve the collection, use, or disclosure of information are done by the business unit that owns the project, process, or system. The business units will consult with the Alberta Health Privacy Team as soon as any changes are anticipated. The Privacy Team will then identify any new privacy impacts that need to be addressed, determine if an amendment is required, and if so, what form it should take. Privacy will do an analysis of what was described in previously submitted PIAs and compare to any implemented change in the project/process.

[138] During the course of our review, we discussed with AH the importance of transparency with respect to building public trust for ABTraceTogether. We provided examples to AH of PIAs for contact tracing apps in other jurisdictions that have been made public to provide transparency (e.g. Australia and New Zealand). We recommended that AH publish its PIA for ABTraceTogether.

[139] On May 7, 2020, AH advised us that:

> A summary of the AB TraceTogether PIA is currently being drafted. It is expected that this summary will be made available to the public after the PIA has been accepted by the OIPC. The summary will include background details relating to the App's development and the public health rationales that support its use in the current pandemic. The summary will also explain how the App works, and how users may opt-out if they decide they no longer wish to use the App or share their data. A summary of the analytics Alberta Health will conduct on aggregate data will also be included. High-level summaries of the privacy and security features of the contracts with IBM and Deloitte will be provided. The summary will also outline details respecting the App's privacy protection features, the risks AH has considered, and the mitigation strategies that are in place to help ensure the privacy of Albertans is being protected.

Findings

- AH completed a PIA and submitted it to the OIPC before implementing ABTraceTogether. We are satisfied that AH and AHS met the requirements of sections

64(1) and 64(2) of HIA. AHS submitted an endorsement letter for the ABTraceTogether PIA.

- We are satisfied that AH has committed to monitor changes to the functionality and implementation of ABTraceTogether, and will submit PIA amendments when required and in compliance with section 64 of HIA.
- We are satisfied with AH's commitment to make public a summary of its PIA.

Recommendations

- We recommend that AH address recommendations made in this report and update its PIA as appropriate. We also recommend AH include AHS in monitoring and reviewing ABTraceTogether such that PIA amendments can be submitted by both custodians in a timely manner.
- We recommend that AH also publish PIA revisions and information concerning compliance with recommendations made in this report, as well as information about the use of the app (e.g. take-up by Albertans) and its effectiveness in meeting stated goals and objectives.

Training for Contact Tracers and Analytics Staff

[140] As part of our review of the PIA, and noting that the purpose of the app is to "[a]ugment… current contact tracing efforts to provide guidance and care to those who are or may be infected", we asked AH for more information about training for contact tracers and analytics staff. More specifically, we asked how they are trained with respect to privacy and security, and applicable ABTraceTogether policies and procedures.

[141] AH described how system access is provisioned and described how management at AH and AHS authorize system access and remove system access to both the contact tracing portal and the contact tracing analytics environment (for more information see Technical Safeguards section below on System Access Controls).

[142] When describing how users are authorized to access the ABTraceTogether portal and how system access is removed, AH said that the same managers who are responsible for authorizing and removing entitlements for access are also "responsible for providing the appropriate training as required." AH described how these same management roles are responsible for authorizing and removing entitlements for access to the analytics environment; however, AH did not say that the managers would be responsible for training the staff who use the analytics environment. Given this, it not clear to us who is responsible for training analytics staff.

[143] The PIA described information flows between AH and AHS in order to support contact tracing through ABTraceTogether. It was not clear to us which positions (i.e. job titles and descriptions) from each organization (i.e. AH and AHS) are involved in contact-

tracing processes and what access is required to perform their job duties. AH clarified the job roles involved with off-boarding, but it remained unclear generally on the positions at AH and AHS and what access to which database(s) they possess.

[144] AH did explain the following with respect to "contact tracers":

> Contract tracers are affiliates of AHS. Currently all of the contract tracers are AHS employees. Retired nurses have been brought back into AHS and their practice licenses have been renewed, they are working as employees to perform contract tracing. There are currently no volunteers; however, volunteers have served as contact tracers. There were medical student volunteers from the University of Calgary and the University of Alberta that were performing the contact tracing function until the middle of May.

[145] AH suggests that employees and volunteers who may not formally hold the title of "contact tracer" may be performing those duties on a temporary basis. In our view, this exposes a potential risk in that these volunteers and reassigned employees may not be sufficiently trained with respect to AH and AHS obligations under the Acts.

[146] With respect to general privacy training, and training specific to ABTraceTogether, AH said:

> Contact tracers complete the mandatory AHS training module that reviews AHS privacy and information security policies and practices. The training is delivered through an online learning module. The information security policy and privacy requirements are also reiterated during training on ABTraceTogether.
>
> There is a three day in class training provided by various subject matter experts to learn the programs and materials required to undertake contact tracing for COVID, including the use of electronic systems. ABTraceTogether is a module in this training. This training includes the policy requirements around confidentiality and information handling associated with ABTraceTogther [sic]. The in class training is followed by scheduled buddy shifts doing the work under peer supervision. Further a competency assessment has been developed to be implemented with all new staff starting at the end of June.

[147] AH described the privacy and security training AHS contact tracers receive. It was not clear to us if contact tracers include those AHS affiliates who work with the analytics data. Therefore, we are not clear if analytics staff at AHS get the same training.

[148] The PIA also described the privacy training that AH staff receive. GoA staff receive internal training, including HIA and FOIP Act training and are required to sign a confidentiality agreement or contract when their employment begins. Staff must adhere to legislation, standards, policies and information management requirements of the GoA. It was not clear to us if specific ABTraceTogether training (which should include the ABTraceTogether policies) is provided to AH staff who use the ABTraceTogether portal or the ABTraceTogether analytics environment.

[149] We also note that the IM Policy (reviewed previously) says that, "Users of the AB TraceTogether Case and Contact Tracing Portal and the Analytics Portal will be presented with an acceptable use policy prior to obtaining access". Despite this, we

have not received confirmation that other project specific policies will be provided to contact tracers and analytics staff.

[150] We reviewed the process contact tracers use when Bluetooth encounter logs are used to contact individuals who have been exposed to someone diagnosed with COVID-19.

[151] We also asked AH what information is provided when communicating with individuals who have been potentially exposed to COVID-19. AH provided excerpts of the phone scripts contact tracers use.

[152] We reviewed the excerpts, and AH confirmed that it only provides the date of exposure, not time of day. The phone script shows that contact-tracing processes have been updated to incorporate ABTraceTogether processes.

[153] We identified the risk that the person being notified may be able to infer who exposed them to COVID-19 depending on what information is disclosed during the notification process. While an individual is only provided with a date, not time of day, there remains a risk that an individual might be able to infer who exposed them to COVID-19 if they are strictly limiting contact with others. We recommend AH make this risk transparent to individuals so they consider this before downloading and using the app.

Findings

- We are generally satisfied with the training that contact tracing and analytics staff receive specific to ABTraceTogether.
- While AH only provides date of exposure and not time, there remains a risk that an individual might be able to infer who exposed them to COVID-19 if they are strictly limiting contact with others.

Recommendations

- We recommend AH clarify how AH and AHS ensure that the ABTraceTogether training is completed and tracked and whether all AH and AHS users of ABTraceTogether are provided access to and training on the four policies provided during the PIA review.
- We recommend AH publicly communicate the risk that an individual might be able to infer who exposed them to COVID-19 if they are strictly limiting contact with others, so individuals can consider this risk before downloading and using the app.

Security in Contracting with Third Parties

[154] An important component of administrative safeguards is ensuring that agreements with third parties are in place and include provisions to protect privacy and ensure security of health and personal information.

[155] With respect to ABTraceTogether, AH confirmed the app is “maintained and governed by AH. AH will also own the solution and manage any data collected by the App”. AH,

however, has agreements with third parties – Deloitte, IBM and Twilio – that are associated with the development, implementation and operation of ABTraceTogether.

[156] Both HIA and the FOIP Act include provisions that place duties and obligations on custodians and public bodies when they enter into agreements with third parties. We reviewed summary information from AH about the agreements between AH and third parties as well as sections from the contracts to assess compliance with the legislative provisions set out below.

Legislative Requirements

[157] Section 1(e) of the FOIP Act defines employee to mean "in relation to a public body, includes a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body".

[158] Section (1)(1)(a) of HIA defines an "affiliate" as, among other things, "a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian" (section 1(1)(a)(iii)), or "an **information manager** as defined in section 66(1) [of HIA]" (section (1(1)(a)(iv)). [emphasis added]

[159] "Information manager" is defined in section 66(1) of HIA:

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

[160] Custodians are required to "enter into a written agreement with an information manager" (section 66(2)) that requires the information manager to comply with HIA, the regulations and the information manager agreement (section 66(5)).

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

[162] Section 7.2 of the HIA Regulation describes what must be included in an information manager agreement.

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

Deloitte

[164] AH says that Deloitte is responsible for "design, development, and deployment of the app and security". Deloitte "will have access to the data during the App development stage, and in support of transition activities to AH."

[165] AH has entered into a service agreement with Deloitte. AH provided us with information about the agreement and provided a copy of the agreement (excluding financials). Among other things, AH said the agreement acknowledges that Deloitte is an "affiliate" of AH and an "employee" as defined in HIA and the FOIP Act respectively, and also that HIA and the FOIP Act apply to health and personal information collected, used or disclosed under the agreement. The agreement requires Deloitte to:

- Make reasonable security arrangements against unauthorized access, use, disclosure, loss, destruction or alteration of health or personal information
- Advise AH of any unauthorized access, use, disclosure, loss or destruction of the health or personal information and provide assistance in breach response
- Comply with HIA and the FOIP Act, and make information available to AH to verify compliance
- Store all health and personal information in Alberta

[166] Deloitte is also prohibited from collecting, using or disclosing health or personal information unless expressly authorized in writing.

[167] As the party responsible for the "design, development, and deployment of the app", Deloitte qualifies as an "information manager" as defined in section 66(1) of HIA (i.e. provides "information technology services").

[168] Therefore, per section 66 of HIA, AH is required to enter into a written agreement with Deloitte and the agreement must require Deloitte to comply with HIA, the regulations and the information manager agreement.

[169] An information manager agreement must also meet the requirements set out in section 7.2 of the HIA Regulation, which says the agreement must, among other things:

- "[I]ndicate whether or not the information manager is permitted to collect health information from any other custodian or from a person and, if so, describe that health information and the purpose for which it may be collected" (section 7.2(b))
- "[I]ndicate whether or not the information manager may use health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be used" (section 7.2(c))
- "[I]ndicate whether or not the information manager may disclose health information provided to it by the custodian and, if so, describe that health information and the purpose for which it may be disclosed" (section 7.2(d))
- Describe the process to respond to access requests and requests to amend or correct health information (sections 7.2(e) and (f))
- Describe how health information provided to the information manager is to be protected, managed, returned or destroyed in accordance with HIA (section 7.2(g))

- Describe how the information manager is to address an expressed wish of an individual relating to the disclosure of that individual's health information, or the process for referring those requests to the custodian (section 7.2(h))
- Set out how an agreement can be terminated (section 7.2(i))

[170] AH stated that its agreements with "Deloitte and IBM contain Alberta Health's standard privacy clauses, which include the necessary provisions to meet its obligations under the *Health Information Act*, including s. 66 and 7.2 of the *Health Information Regulation*". AH also provided a copy of its agreement with Deloitte and provided a summary that identified the sections of the contract that demonstrated compliance with HIA and the HIA Regulation requirements.

[171] In our view, after reviewing the contract between the Minister of Health and Deloitte, it appears that AH has met the requirements set out in section 66 of HIA and section 7.2 of the HIA Regulation.

IBM

[172] AH says that, "The App will use AH's IBM-based infrastructure, and only Canadian-resident services and infrastructure will be used."

[173] AH says it has contracted with IBM for "data storage and application penetration testing". The ABTraceTogether portal and analytics databases are managed by IBM. AH stated, "App data will be kept on IBM servers located in Montreal". AH also described that, "The analytics database sits within the IBM Cloud Service. The infrastructure and server support is provided by IBM."

[174] AH provided the relevant parts of its managed operations agreement with IBM as well as the relevant schedules for our review. This agreement described how IBM provides information technology (IT) services to AH and includes privacy and confidentiality provisions in the contract.

[175] AH described its "Cloud Services Agreement" with IBM and provided the following about the agreement:

> IBM, its affiliates, and contractors of either, may access and use the Content solely for the purpose of providing and managing the Cloud Service. IBM will treat all Content as confidential by not disclosing Content except to IBM employees and contractors and only to the extent necessary to deliver the Cloud Service.
>
> IBM will return or remove Content from IBM computing resources upon the expiration or cancellation of the Cloud Service, or earlier upon Client's request.

[176] When the PIA was submitted, AH said, "This Agreement has not been finalized. The agreement is a Change Order to the existing Managed Ops agreement with IBM". To date, AH has not confirmed if the agreement has been finalized.

[177] As an IT services provider, IBM appears to qualify as an "information manager" as defined in section 66(1) of HIA (i.e. "stores, retrieves or disposes of health information", provides "information technology services").

[178] Therefore, per section 66 of HIA, AH is required to enter into a written agreement with IBM and the agreement must require IBM to comply with HIA, the regulations and the information manager agreement.

[179] As mentioned above in the section on the Deloitte contract, AH stated that its agreements with "Deloitte and IBM contain Alberta Health's standard privacy clauses, which include the necessary provisions to meet its obligations under the *Health Information Act*, including s. 66 and 7.2 of the *Health Information Regulation*". AH provided a copy of its managed operations agreement and a summary of how this agreement meets the requirements of HIA and the HIA Regulation.

[180] With respect to storing and using health information outside Alberta, section 8(4) of the HIA Regulation says the custodian must enter into a written agreement that, among other things:

> (a) provides for the custodian to retain control over the health information,
> (b) adequately addresses the risks associated with the storage, use or disclosure of the health information,
> (c) requires the person to implement and maintain adequate safeguards for the security and protection of the health information,
> (d) allows the custodian to monitor compliance with the terms and conditions of the agreement, and
> (e) contains remedies to address any non-compliance with or breach of the terms and conditions of the agreement by the other person.

[181] In our view, it appears that AH has met the requirements set out in section 66 of HIA and sections 7.2 and 8(4) of the HIA Regulation, with respect to the contract with IBM. However, AH has not confirmed that its change order has been finalized. We recommend AH to confirm with us when its change order has been finalized.

Twilio

[182] AH says that it "has subcontracted through IBM with Twilio for services relating to information processing and SMS messaging. Twilio redacts the entirety of the message body and the last four digits of the user's phone number. Twilio uses Amazon Web Services servers, located in the United States of America."

[183] We have already said IBM is an information manager to AH; Twilio is a subcontractor to IBM and provides information processing. Twilio therefore appears to qualify as an "information manager" as defined in section 66(1) of HIA.

[184] Per section 66 of HIA, AH is required to enter into a written agreement with Twilio and the agreement must require Twilio to comply with HIA, the regulations and the information manager agreement.

[185] An information manager agreement must also meet the requirements set out in section 7.2 of the HIA Regulation (previously summarized).

[186] As mentioned earlier, AH stated that it subcontracted through IBM with Twilio for services; therefore, it is our understanding that AH does not have an agreement directly with Twilio but is relying on its agreement with IBM as well as the agreements between IBM and its subcontractors.

[187] In response to our request for additional information on how AH meets the requirements set out in section 66 of HIA and sections 7.2 and 8(4) of the HIA Regulation, AH provided the contract between AH and IBM which includes details on how IBM shall bind subcontractors to the terms and conditions of the contract between AH and IBM.

[188] AH provided several details on how its contract with IBM includes information management and other responsibilities for IBM's subcontractors. AH also provided us with information about Twilio's "Terms of Service", and the "Data Protection Addendum" that forms part of them (but we did not receive copies of Twilio's "Terms of Service" for review). AH says these generally:

- Authorize Twilio to "process personal data as necessary to provide the Services under the Agreement"
- State that Twilio "does not sell Customer's personal data or Customer end users' personal data and does not share such end users' information with third parties for compensation or for those third parties' own business interests"
- Set out the circumstances in which personal data transferred to Twilio may be disclosed
- Address termination of the agreement, including the return and destruction of "Customer Content"

[189] Section 8(4) of the HIA Regulation says a custodian must enter into a written agreement with a person that is storing or using information outside of Alberta.

[190] In describing how it has met compliance with section 8(4) of the HIA Regulation, AH said, "Alberta Health has met the requirements of section 8(4) of the Health Information Regulation in its contract with IBM, and the same substantive protections exist in the subsequent contractual arrangement with Twilio."

[191] We have reviewed the agreement between AH and IBM and the clauses that require IBM to bind its subcontractors to the terms and conditions of its contract with AH. However, without reviewing the "Terms of Service" or excerpts from the agreement between IBM and Twilio, we are unable to verify if that agreement complies with the contract between IBM and AH, and therefore the requirements set out in section 66 of the HIA and sections 7.2 and 8(4) of the HIA Regulation, with respect to the services provided by Twilio.

Findings

- Deloitte is an information manager to AH. In our view, after reviewing the contract between the Minister of Health and Deloitte, it appears that AH has met the requirements set out in section 66 of HIA and section 7.2 of the HIA Regulation.
- IBM is an information manager to AH. In our view, it appears that AH has met the requirements set out in section 66 of HIA and sections 7.2 and 8(4) of the HIA Regulation, with respect to the contract with IBM. However, AH has not confirmed that its change order has been finalized.
- IBM subcontracts Twilio for information processing services. Twilio is an information manager to AH. It is not clear from the information provided to us that the requirements set out in section 66 of HIA and sections 7.2 and 8(4) of the HIA Regulation have been met with respect to the services Twilio provides.

Recommendations

- We recommend AH to confirm with us when its change order with IBM has been finalized.
- We recommend that AH provide us with additional information to confirm that the agreement meets requirements set out in section 66 of HIA and sections 7.2 and 8(4) of the HIA Regulation, with respect to the services Twilio provides.

Technical Safeguards

[192] AH's PIA included a privacy risk table that highlighted the privacy risks associated with ABTraceTogether and how it has mitigated risks. AH identified risks such as unauthorized use of health or personal information by internal or authorized parties, unauthorized collection, use or disclosure of health or personal information by external parties, loss of integrity of information and loss, destruction or loss of use or availability of information.

[193] The mitigation strategies included administrative and technical safeguards. In this section, we will focus on the technical details provided by AH to protect personal and health information involved in ABTraceTogether.

System Access Controls

[194] AH described system access controls specific to ABTraceTogether, including role-based access, clearly defined access authorization and administration procedures, and secure authentication. For example:

- AH confirmed that, "Access to the Contact Tracing Portal is limited to Alberta Health and AHS contact-tracing staff with appropriate permissions based on existing Alberta Health and AHS provisioning processes and procedures." AH provided a detailed description of the AH and AHS access provisioning processes and procedures, including approvals from directors and managers in relevant program areas. AH also outlined the process to remove access permissions.

- The PIA included a system access roles table describing types of user roles, description of the role, approximate number of users in that role, the type of access and the type of information accessed. We asked AH to provide additional details to clarify how the user roles work with respect to the two systems (portal and analytics environment) and which organization has these roles. For example, the PIA referred to AH contact tracers but then AH described that contact tracers are AHS employees. The PIA only has two types of user roles for AH and AHS affiliates and they are "contact tracers" and "back-end/server side administrators".

- AH described how it mitigates the risk of unauthorized access to the system by stating that "access to the… portal is locked down at the firewall to only permit access from [AH] and [AHS] subnets and IP addresses."

- AH appears to have implemented segregation of duties. AH said, "[N]o one [at AH and AHS] has simultaneous access to both the operational and analytics databases."

[195] AH described how risks related to allowing users to access the system remotely are mitigated, "Users accessing [the contact tracing portal] from a remote location must first VPN into their organization networks using multi-factor authentication (MFA)" and

"log-in requests [are directed] to the AHS Active Directory for authentication and confirmation of provisioned entitlements."

Finding

- In our view, AH described reasonable system access controls, security measures and authorization processes necessary to protect and limit access to health and personal information. Further, AH has demonstrated consideration for the privacy principles of limited access and access on a "need to know basis".

Securing Data in Transit and Data at Rest

[196] AH stated in its PIA that the "App relies on anonymized IDs, and transmission of phone number is encrypted. Only AH staff will be able to decrypt the data".

[197] AH provided details on its infrastructure architecture and described how the cryptographic key management services works, how the keys are protected and where the decrypted data elements are stored.

[198] AH stated that, "Temporary IDs will be stored in an encrypted form on users' smartphones and will be periodically refreshed."

[199] AH described the following encryption protocols in place to protect data in transit:

- All user access to the contact tracing and analytics web application is protected by TLS 1.3 cipher suites (minimum client-side requirement of TLS 1.2)
- The remote API call to contact tracing application web services from mobile App is protected by TLS 1.3 cipher suites (minimum client-side requirement of TLS 1.2)
- All access from front-end web applications to back-end DB2 databases are protected by TLS 1.3 cipher suites (minimum client-side requirement of TLS 1.2)
- Data sharing between contact tracing and analytics environments is protected by TLS 1.3 cipher suites (minimum client-side requirement of TLS 1.2)

[200] The analytics environment is in Montreal on a server managed by IBM. The server that creates the "Hashed User ID" stored in the analytics environment "is not accessible by the analysts who have access to the analytics environment" further reducing the potential to re-identify a user via the analytics database. This is also discussed in the section below on de-identification.

[201] Data extracts pushed into analytics platform are de-identified (i.e. hashed) using an algorithm currently accepted as cryptographically secure.

[202] In our view, hashing the user ID, combined with AH and AHS staff not having access to both portal and analytics environments, are reasonable controls to reduce the likelihood of re-identifying a user. We recommend that AH consider further obfuscating user IDs through the use of "salting".

[203] AH described the following controls in place to protect health and personal information in the databases:

- "Exposure logs, user ID, and phone number are not encrypted at rest on databases. The databases are specific to the ABTraceTogether solution. The solution is further configured to limit traffic to known network and monitored for any unexpected traffic. Administrative controls, physical security measures, logical access controls, logging and monitoring are in place for Alberta Health data centres, front-end applications and back-end databases to prevent and detect unauthorized access from Alberta Health users, Alberta Health Services (AHS) contact tracers and IBM support staff. Exposure logs are stored in Alberta Health data centres for 21 days, while exposure logs older than 21 days are automatically removed from the solution as they are no longer needed for the purpose of COVID-19 contact tracing."

- "The database servers are hardened using secure engineering practices (e.g. remove and disable unneeded accounts and features, segregation of duties, enforcing password rules in alignment with GoA Password Standard, TLS encryption of connections, separate instances, and logging and auditing). The IBM cloud infrastructure used by Alberta Health has administrative, physical and logical security measures in place that meet Alberta Health security requirements as well as demonstrating compliance to established organizational frameworks and controls…"

[204] The PIA described how AH has "back-end controls protecting data including backups".

[205] The PIA described mitigation of risks by the "completion of security threat risk assessments, vulnerability testing, and penetration testing. Issues identified with medium or higher security risks were reviewed and mitigated in advance of production deployment; remaining risks will be monitored."

[206] In our view, AH has implemented reasonable compensating controls (e.g. limiting traffic to known networks, requiring a VPN and strict access controls) to mitigate some risks of not encrypting data at rest. However, we recommend that AH implement encryption for data at rest, especially for the operational database that stores user ID and phone number pairings.

Finding

- In our view, AH described reasonable controls in place to protect data in transit and data at rest.

Recommendations

- Despite finding that reasonable controls are in place to protect data in transit and data at rest, we recommend AH to consider further obfuscating user IDs through the use of "salting".

- We also recommend that AH implement encryption for data at rest, especially for the operational database that stores user ID and phone number pairings.

Monitoring and Auditing

[207] With respect to monitoring and auditing access, the PIA originally submitted by AH said:

> The App does not include functionality that requires logging for the purpose of identifying an individual's access to information. However, access to data submitted by App users is strictly limited to contact tracers or database administrators, both of whose access to the data is logged and governed by legislation and the terms of their employment with the Government of Alberta. As the rollout of AB Trace proceeds, Alberta Health will commit to developing and implementing an audit strategy that will address any emerging issues.

[208] During the PIA review process, AH provided additional information as follows:

- "The audit strategy is expected to be developed by the end of May with the implementation following in June. Alberta Health is still exploring potential audit approaches, the discussions to date have centered on adopting a randomized audit follow up, selecting at random users activity for review [sic]. Alberta Health would pull an audit report and return this to Alberta Health Services for review and follow up with particular contact tracers."

- "The AB TraceTogether Contact Tracer Web Application is developed to comply with the Provincial Logging and Auditing Standard (version 1.4). Specifically, the logs capture the following information:

    - The Contact Tracer ID
    - A timestamp capturing date and time
    - The action taken in the web app
    - The ID of the user record that the Contact Tracer is interacting with
    - The user IDs of the information which is being viewed."

- "Auditing will include the analytics environment which captures logs that meet the Provincial Logging and Audit Standard. The auditing approach will consist of randomly selected users for audit as well as any incident or complaint driven audits."

[209] AH provided an update on its auditing program stating, "The auditing program has been developed and will be evolved in response to any insights uncovered as a part of its implementation. Alberta Health had targeted auditing to start in June, based on low App downloads and the number of users uploading their exposure logs being low, the access audit has been rescheduled for July."

[210] Further, AH explained that, "Alberta Health collects information directly from Albertans through the ABTraceTogether application. This information is then disclosed to AHS for

contact-tracing purposes only. The current volume of users and exposure uploads has resulted in a delayed start to the auditing of accesses."

Finding

- AH will be implementing its audit strategy in July 2020. We find AH has addressed monitoring and auditing in a reasonable manner.

Recommendation

- We recommend AH provide us with an update on its audit strategy after implementing the strategy.

Data Accuracy and Integrity

[211] Section 61 of HIA states, "Before using or disclosing health information that is in its custody or under its control, a custodian must make a reasonable effort to ensure that the information is accurate and complete."

[212] Section 35(a) of the FOIP Act states, "If an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body must… make every reasonable effort to ensure that the information is accurate and complete."

[213] AH's PIA identified "[l]oss of integrity of information" as a potential privacy risk associated with ABTraceTogether. AH was specifically referring to "corruption of data before or during transfer of data between users, or between users and AH".

[214] We were also concerned about individuals potentially uploading Bluetooth encounter logs without having received a positive diagnosis, thus risking that other users might be contacted by AHS, despite no increased risk of exposure. A related risk concerns the potential for AHS staff to misinterpret encounter logs and contact individuals who do not meet the threshold (i.e. within two metres, for 15 minutes or more).

[215] To mitigate these risks, AH advised us that, "Data transferred from users to AH requires confirmation via SMS code and is limited to anonymized IDs and phone numbers." More specifically, before an individual can upload their Bluetooth encounter logs to AH, "The application will send/display a code via SMS that is verified by both a contact tracer from AH [sic], and the user." AHS stated that this process "[e]nsures that all calls from the App are authenticated to a registered user."

[216] AH also provided additional details on how contact tracers interpret the Bluetooth encounter logs that are uploaded voluntarily by a user who has been diagnosed with COVID-19. AH said:

> Exposures lasting 15 minutes or more at a distance of 2 meters or closer are identified for the contact tracers to follow up on. The requirement for 15 minutes of exposure at a distance of two meters or closer is based off of the current clinical guidance available. Based on revised guidance this exposure requirement may change in the future. There is also discretion that can be exercised by the Contact Tracer based on their discussion with the individual who has tested positive to help determine who of the contacts may have exposure risk.

[217] AH also said:

> The app uses Received Signal Strength Indicator (RSSI) readings to determine if app users have been within approximately 2 meters of each other. The app uses successive communications to estimate the duration of an encounter. The app will complement contact tracing and is not a substitute for professional judgement and human involvement in contact tracing.

Findings

- The technical control requiring that the application send or display a code via SMS that is verified by both a contact tracer and AHS is a reasonable mitigation to prevent unauthorized uploading of Bluetooth encounter logs.
- Having contact tracers assess a user's exposure risk by combining information and experience from traditional contact-tracing processes with Bluetooth encounter log information is a reasonable control to reduce the risk of false-positive encounters, and aligns with the purpose of the app.

De-identifying Information in the Analytics Environment

[218] As previously described, if a user tests positive for COVID-19 and consents to having their Bluetooth encounter logs uploaded, a de-identified version of the logs is also uploaded to the ABTraceTogether analytics environment.

[219] AH said it will conduct analytics on "aggregated App data to track performance indicators and App functionality".

[220] Key performance indicators and metrics include the "number of contacts, time between contacts, duration of exposure, distance/proximity of contacts, phone number area codes, tracing performance, number of temporary ID changes, number of application downloads and deletions."

[221] AH said, "The analysis of data will help contact tracers map… the total number of positive cases identified, the number of users who have been contacted but not tested… and the number of users who have not been contacted."

[222] Further, analytics will "provide insight into opportunities to tune" multiple aspects of ABTraceTogether's functionality to "ensure it remains as accurate and useful as possible."

[223] We were concerned about the potential of identifying an individual from the information in the analytics environment. We noted that AH has the mobile number and user ID in the portal and the analytics environment contains user ID with the Bluetooth encounter log details. We asked AH how it mitigates the risk of being able to identify someone from the logs in the analytics environment.

[224] AH said that user IDs are a necessary structural component in its analytics environment. However, to reduce the risk of re-identification (i.e. linking user IDs to a mobile number which may still be in the operational database), user IDs are "hashed". Hashing is a one-way process that generates a structured output based on arbitrary inputs. In context, hashing a user ID would create a "hash value" that is difficult to reverse and subsequently match to a phone number in the operational database. As mentioned earlier in the section on "Securing Data in Transit and Data at Rest", we recommend that AH consider further obfuscating user IDs through the use of "salting".

[225] AH said it "can confirm that no one has simultaneous access to both the operational and analytics databases. In addition to this anonymity is preserved as the identifiers from the operational database are not directly copied to the analytics database. The analytical environment uses a Hashed User ID rather than the User ID. This results in an additional layer of abstraction protecting the data and reducing the risk of identification. No identifiable information is copied into the analytics environment."

Finding

- We are satisfied that hashing, combined with not allowing staff access to both the operational and analytical databases, are sufficient to limit the risk of re-identification.

Withdrawal from Participation and Off-Boarding

[226] AH's PIA says, "Users who decide they no longer want to share their data may opt out at any time." AH informs users of this option through the privacy notice, the privacy statement and the online FAQ document.

[227] We found that full withdrawal from participating in ABTraceTogether requires users to take the following two steps:

- Delete the application to stop tracing functionality
- Email hiahelpdesk@gov.ab.ca to remove the collected phone number[16]

[228] We found that some users may incorrectly assume only the first step (i.e. uninstalling ABTraceTogether) is sufficient to cease participation and de-identify any information AH may have collected. While users who uninstall the application would no longer be broadcasting temporary IDs over Bluetooth, they would still be "registered" on ABTraceTogether. As a result, they would be identifiable via their phone numbers and could be reached by contact tracers should their temporary IDs be uploaded by an app user who is diagnosed with COVID-19 and consents to uploading their Bluetooth encounter log (if captured within relevant retention periods).

[229] In our view, without thoroughly reviewing the notice, privacy statement or FAQ, users would likely be unaware a second step (i.e. contacting the HIA Helpdesk) is necessary to remove their phone number from the database.

[230] We also noticed inconsistencies in the documentation on off-boarding. We found that the FAQ and privacy statement inconsistently state what information is deleted upon withdrawal of participation. In one document, AH states that both phone number and user ID are deleted. In another document, it states that only a user's phone number is removed.

[231] AH confirmed that only phone numbers are deleted, which de-associates a registrant's phone number from their corresponding user ID upon full withdrawal from ABTraceTogether. The remaining records (e.g. de-associated user ID) would be deleted following AH's established retention schedule.

[232] AH provided additional detail on who is involved in the off-boarding process when ABTraceTogether users no longer want to participate.

[233] Users email hiahelpdesk@goa.ab.ca to request withdrawal from participation, including their phone number. AH follows up with the user and confirms whether they want to withdraw from ABTraceTogether. Contact tracers are then notified when an individual's request for withdrawal has been confirmed, and the contract tracer off-boards the user. AH said, "Once the user's phone number is deleted from the database, any remaining

[16] Contact tracers can also remove mobile number when they are talking to someone regarding a contact.

user data becomes anonymized and unsearchable. Any remaining anonymized data will be deleted from the system via the automated rolling deletion process every 21 days."

[234] The user off-boarding function for ABTraceTogether is performed by contact tracers.

Findings

- In our view, some users may incorrectly assume only the first step (i.e. uninstalling ABTraceTogether) is sufficient to cease participation and de-identify any information AH may have collected. Without thoroughly reviewing the notice, privacy statement or FAQ, users would likely be unaware a second step (i.e. contacting the HIA Helpdesk) is necessary to remove their phone number from the database.
- We also found that the FAQ and privacy statement inconsistently state what information is deleted upon withdrawal of participation. In one document, AH states that both phone number and user ID are deleted. In another document, it states that only a user's phone number is removed.

Recommendation

- We recommend that AH review its public documents to ensure they are clear that only the phone number is deleted when a user withdraws participation, not the user ID.

Retention of Personal and Health Information

[235] Section 35(b) of the FOIP Act states:

> **35** If an individual's personal information will be used by a public body to make a decision that directly affects the individual, the public body must…
>
> (b) retain the personal information for at least one year after using it so that the individual has a reasonable opportunity to obtain access to it, or for any shorter period of time as agreed to in writing by
>
> (i) the individual,
> (ii) the public body, and
> (iii) if the body that approves the records and retention and disposition schedule for the public body is different from the public body, that body.

[236] HIA does not include provisions specific to retention of health information. However, pursuant to section 108(1)(o) of HIA, "The Lieutenant Governor in Council may make regulations… respecting the retention, disposal and archival storage of records for the purposes of ".

[237] At this time, there are no regulations made under HIA that prescribe length of retention for health information. Some custodians may be required to comply with records retention directives or policies issued by their professional colleges.

[238] Despite there being no legal requirements under HIA or the FOIP Act to limit the retention of health or personal information, AH provided us with information concerning the retention of health and personal information collected via ABTraceTogether.

[239] More specifically, AH said:

> Data older than 21 days is removed from the user's smartphone via automated rolling deletion. Data uploaded to the server is deleted after 21 days via automated rolling deletion. Deletion of the application also results in the removal of the stored data from the user's smartphone.

[240] Further:

> The information in the analytics environment will be maintained for 18 months post the pandemic. After this 18 month period the analytics database will be deleted. The reports and assessments generated from this information will be maintained with the Alberta Health and Alberta Health Services record retention schedules. The source code for the applications used will be maintained in case there is a need in the future pandemic.

[241] With respect to the requirement of section 35(b) of the FOIP Act, AH said:

> Section 35(b) applies only if an individual's personal information will be used by a public body to make a decision that directly affects the individual. FOIP applies to phone numbers that are not uploaded and linked to health information. Alberta Health is not using those phone numbers

to make a decision that directly affects the individual. Therefore, the duties in section 35 of FOIP do not apply in this situation.

[242] We accept AH's position on section 35(b) of the FOIP Act.

[243] We also requested information concerning the retention of information used to contact someone who has potentially been exposed, and where that information is recorded (i.e. ABTraceTogether databases or another system) and for how long this information is retained. AH clarified that data from ABTraceTogether will not be stored in a patient's medical record; however, we continue to have questions about "data [that] will be compiled with information from other systems" (see "Data Matching" section above).

Finding

- AH has considered the principle of limiting retention by retaining records for only as long as necessary to fulfill the purposes established.

Recommendation

- We recommend AH provide information concerning the retention of information used to contact someone who has potentially been exposed, and where that information is recorded and for how long it is retained.

Decommissioning ABTraceTogether

[244] When the COVID-19 pandemic passes, the impetus for collecting information through ABTraceTogether to address the public health threat may no longer be present.

[245] AH's online FAQ says that, "Once contact tracing for COVID-19 ceases, we will prompt users [sic] disable Alberta Contact Tracing's functionality."

[246] We asked for more detail on how AH planned to decommission the app and described some potential privacy and security risks that may occur if the app is not properly decommissioned, including the possibility of exploitation (e.g. tracking) of devices which may continue to broadcast expired Bluetooth tokens.

[247] AH recognized that it had not addressed decommissioning, and indicated that its priority had been to deploy the app. AH has since committed to dismantling ABTraceTogether after the COVID-19 pandemic has passed. AH said:

> The App would continue to scan for other Apps and advertise that it is active but would no longer exchange IDs. There is a risk that in this state an exploit could be developed. Alberta Health expects communication around winding down the App will mitigate the risk that individuals do not delete the App and continue to have it active. As part of a point release, brining [sic] the App to version 1.1, functionality to remotely disable the App will be introduced. This functionality will effectively mitigate the risk by enabling the App to be disabled. Once disabled the App will not exchange Temporary IDs nor attempt any communication via Bluetooth.

[248] As previously stated, AH described "the information exchanged between users relies upon Temporary IDs generated by an algorithm running on the servers, with the servers disabled, even if a user keeps the app on their phone, it will run out of Temporary IDs to exchange and cease to function."

[249] In addition, AH committed to "send[ing] out a notification to all registered users via SMS that the app is no longer required and should be delete." AH added that it "will shut down the back end servers making it impossible to register for the App or receive data from users."

[250] As noted previously, AH said that anonymized information in the analytics environment will be retained for 18 months after the end of the pandemic.

Finding

- It is our view that dismantling the app is a critical measure to protect the privacy of Albertans.

Recommendation

- We recommend that AH engage with the OIPC when it is time to dismantle the application, and provide an update on its decommissioning plans publicly.

Functionality

[251] The ABTraceTogether app is built upon the BlueTrace and OpenTrace protocol, and therefore it introduces users to security risks, as detailed in the BlueTrace white paper. Two items are particularly noteworthy:

- Using the app on iOS devices
- Risks to geolocation information when the app is run on Android devices

Using ABTraceTogether on iOS devices

[252] Apple restricts the use of certain types of background Bluetooth activity. As a result, in order for ABTraceTogether to function as desired, AH advises iOS users to run the app in the foreground and leave the phone screen unlocked.

[253] In our view, leaving iOS devices unlocked represents a significant security risk for individuals running the app. For example:

- If a person's phone is stolen, the "last line of defence" that a passcode lock provides is rendered useless
- Some organizations provide Apple devices to employees and require them to follow certain acceptable use policies to protect sensitive corporate records; leaving a device unlocked introduces unmitigated security risks[17]

[254] AH stated that with respect to the "[i]ssue with employees running app [sic] on 'enterprise-issued' devices that store or make other health or personal information accessible" that "[t]hese are organizational decisions that will be governed by the acceptable use policies for an organization's assets."

[255] We asked AH if it had any timelines to mitigate the Apple issue. On May 7, 2020, AH advised us that:

> Alberta Health is actively working with both Apple and Google to take advantage of enhancements to the operating systems expected to be released by both companies in the next month to support the response to COVID-19. Alberta Health recognizes the usability and security risks associated with the Apple iOS foreground issue and has communicated this to Apple. When Apple releases a fix that meets Alberta Health's requirements, Alberta Health and its developer partners will adopt, test and review the functionality. Given the dependencies involved a specific timeline can not yet be provided.

[256] More recently, Apple and Google announced their partnership to create an "Exposure Notification Framework" which would resolve the need to run ABTraceTogether in the foreground on Apple devices. The framework became available in May 2020.

---

[17] It is unclear if mobile device management (MDM) policies deployed to iOS devices are paramount to the always-running foreground state that ABTraceTogether places an iPhone in, potentially placing these managed devices in contravention of corporate policies.

[257] On May 28, 2020, AH advised us that:

> Alberta Health has advised the public through its Frequently Asked Questions content, to secure their phone when running the App, in a safe location, such as a pocket. Alberta Health has received many inquiries from the public on the iOS foreground issue demonstrating awareness of the privacy and security risks as well as the impact on usability. Alberta Health is actively working on a version 2 release of the ABTraceTogether App which will take advantage of the enhancements offered by Google and Apple and address the iOS foreground risks. Specifically it will enable iPhones to support contact tracing in the background. Subject to successful development and the completion of testing it is expected that version 2.0 may be available as early as the second week of June. As part of the plan for the second release of the ABTraceTogether App Alberta Health is undertaking an amendment to the Privacy Impact Assessment. It is expected that the PIA amendment will be the means by which Alberta Health updates your office regarding the enhancements to the App and associated risk mitigation activities.

[258] To date, we have not formally received any additional information from AH concerning this issue.

Risks to Geolocation Information on Android Devices

[259] Android users are prompted to grant the app permission to access location information during the initial setup on their devices. This prompt is the result of the Android operating system defining Bluetooth broadcasting and scanning as a form of "fine location" information, along with GPS and cellular location data. As such, the app is technically capable of accessing these "fine location" records, and further, the permission notification may be a source of concern for some users.

[260] AH has taken steps to mitigate this risk by publishing information for users in its online FAQ, under the heading "Privacy" and "Why does the AB TraceTogether app need Location Permission on Android?". This document confirms that ABTraceTogether running on Android devices does not "capture or use information about your location" and provides a link to a webpage.[18]

[261] To further mitigate this risk, we note, on May 15, AH published the ABTraceTogether source code to provide the opportunity for the public and security researchers to validate that GPS or cellular location information is not collected or used.[19]

Findings

- Overall, we acknowledge that AH has taken steps to mitigate risks to individuals running ABTraceTogether on iOS and Android devices. These steps may be sufficient for users who voluntarily choose to run ABTraceTogether on their personal smartphones. Individuals are not subject to Alberta's privacy laws, and have no legal obligations to

[18] The webpage is available at https://developer.android.com/guide/topcs/connectivity/bluetooth.
[19] The source code is available at https://github.com/abopengov.

safeguard their own personal information. We nonetheless recommend that individuals review the materials AH has made public as well as other resources, so that they can make an informed choice to run the app with full knowledge of potential risks to privacy.

- In our view, the risk mitigation that AH has put in place (i.e. public information for users with directions to reduce risk) is not sufficient with respect to employees who may be running ABTraceTogether on enterprise-issued devices (i.e. issued by regulated public bodies, custodians or private sector organizations) that store or make other health or personal information accessible.

  That is, public bodies, custodians and private sector organizations have legal obligations under Alberta's FOIP Act, HIA and *Personal Information Protection Act*, respectively, to make reasonable security arrangements to protect health and personal information in their custody or control. The risks represent a potential contravention of Alberta's privacy laws by regulated entities if they were to allow employees or affiliates to run the app on enterprise-issued devices that store or make other health or personal information accessible.

Recommendations

- We recommend that AH continue to make information available to users concerning how the functionality issues contribute to privacy risks for individuals.
- We recommend AH continue to make available the ABTraceTogether source code, and to commit publicly to publishing updated versions of the source code.
- We recommend AH continue to liaise with the necessary parties to arrive at a solution for the security limitations, and to submit a PIA amendment should such changes occur.

Summary of Findings

[262] The following is a list of findings from our PIA review of ABTraceTogether:

Health and Personal Information

- Data elements collected, used and disclosed through ABTraceTogether are both health information to which HIA applies, and personal information to which the FOIP Act applies.

Authority to Collect, Use and Disclose Health and Personal Information

- The PIA establishes that AH and AHS have legal authority to collect, use and disclose health and personal information in ABTraceTogether.

Authority for Indirect Collection

- The PIA establishes that AH and AHS have legal authority to collect health information indirectly pursuant to section 22(2)(a) (indirect collection authorized by the individual) and section 22(2)(d) (direct collection not reasonably practicable).

Notice

- Information provided through the Google Play Store and Apple App Store refers to Bluetooth encounter logs that are retained for "14 days", which is inconsistent with information AH provided in its PIA, and our understanding of how the app functions (i.e. contacts are logged for 21 days).
- There are a number of inconsistencies between information included in the privacy notice, FAQ and privacy policy with the information included in the PIA's legal authority table.
- It would not be clear to users of the app that "all" of the "handshakes" that occur are logged, given the app has generally been described publicly as recording encounters that are two meters or closer and a minimum of 15 minutes in duration.

Consent

- AH and AHS have the legal authority to collect, use and disclose health and personal information through ABTraceTogether without relying on consent. AH has decided that a consent-based approach provides Albertans with more choice and control.
- The voluntary nature of the app and the consent-based approach by AH is consistent with the privacy principle that individuals are able to control how their personal information is collected, used and disclosed. The consent AH is using, however, does not meet the requirements of HIA or the FOIP Act, potentially causing confusion.

Limited Collection, Use and Disclosure

- There are challenges to technically limiting the over collection of Bluetooth encounter logs or "handshakes" at distances greater than two metres, due to the nature of the technologies (i.e. Bluetooth, BlueTrace protocol) involved. Therefore, the collection of all handshakes, not only those within two metres, may not meet the requirement in HIA to collect (by AH) or disclose (to AHS) "only the amount of health information that is essential to enable the custodian… to carry out the intended purposes" (section 58).

Data Matching

- It is not clear whether data matching is taking place, specifically in relation to CDOM and other medical record systems.

Organizational Privacy Management

- The OIPC has previously accepted AH's Organization Privacy Management PIA.
- AHS submitted an updated Organization Privacy Management PIA in November 2019 that has not yet been accepted.

Project Specific Policies and Procedures

- AH has developed reasonable project specific policies for ABTraceTogether.
- There is a risk that information collected through ABTraceTogether could be used for quarantine enforcement. In addition to other project specific acceptable use policies, AH developed a policy that prohibits the use of information for quarantine enforcement. "IM Policy 030 Use of AB TraceTogether Not Authorized for Quarantine Enforcement" policy is an acceptable risk mitigation measure.

Risk Assessment (PIA Compliance)

- AH completed a PIA and submitted it to the OIPC before implementing ABTraceTogether. AH and AHS met the requirements of sections 64(1) and 64(2) of HIA. AHS submitted an endorsement letter for the ABTraceTogether PIA.
- AH has committed to monitor changes to the functionality and implementation of ABTraceTogether, and will submit PIA amendments when required and in compliance with section 64 of HIA.
- AH has committed to make public a summary of its PIA.

Training for Contract Tracers and Analytics Staff

- Generally satisfied with the training that contact tracing and analytics staff receive specific to ABTraceTogether.

- While AH only provides date of exposure and not time, there is still a risk that an individual might be able to infer who exposed them to COVID-19 if they are strictly limiting contact with others.

Security in Contracting with Third Parties

- Deloitte is an information manager to AH. It appears that AH has met the requirements set out in section 66 of HIA and section 7.2 of the HIA Regulation.
- IBM is an information manager to AH. It appears that AH has met the requirements set out in section 66 of HIA and sections 7.2 and 8(4) of the HIA Regulation, with respect to the contract with IBM. However, AH has not confirmed that its change order has been finalized.
- IBM subcontracts Twilio for information processing services. Twilio is an information manager to AH. It is not clear from the information provided that the requirements set out in section 66 of HIA and sections 7.2 and 8(4) of the HIA Regulation have been met with respect to the services Twilio provides.

System Access Controls

- AH described reasonable system access controls, security measures and authorization processes necessary to protect and limit access to health and personal information. Further, AH has demonstrated consideration for the privacy principles of limited access and access on a "need to know basis".

Securing Data in Transit and Data at Rest

- AH described reasonable controls in place to protect data in transit and data at rest.

Monitoring and Auditing

- AH will be implementing its audit strategy in July 2020. AH has addressed monitoring and auditing in a reasonable manner.

Data Accuracy and Integrity

- The technical control requiring that the application send or display a code via SMS that is verified by both a contact tracer and AHS is a reasonable mitigation to prevent unauthorized uploading of Bluetooth encounter logs.
- Having contact tracers assess a user's exposure risk by combining information and experience from traditional contact-tracing processes with Bluetooth encounter log information is a reasonable control to reduce the risk of false-positive encounters, and aligns with the purpose of the app.

De-identifying Information in the Analytics Environment

- Hashing, combined with not allowing staff access to both the operational and analytical databases, are sufficient to limit the risk of re-identification.

Withdrawal from Participation and Off-Boarding

- Some users may incorrectly assume only the first step (i.e. uninstalling ABTraceTogether) is sufficient to cease participation and de-identify any information AH may have collected. Without thoroughly reviewing the notice, privacy statement or FAQ, users would likely be unaware a second step (i.e. contacting the HIA Helpdesk) is necessary to remove their phone number from the database.
- The FAQ and privacy statement inconsistently state what information is deleted upon withdrawal of participation. In one document, AH states that both phone number and user ID are deleted. In another document, it states that only a user's phone number is removed.

Retention of Personal and Health Information

- AH has considered the principle of limiting retention by retaining records for only as long as necessary to fulfill the purposes established.

Decommissioning ABTraceTogether

- Dismantling the app is a critical measure to protect the privacy of Albertans.

Functionality

- AH has taken steps to mitigate risks to individuals running ABTraceTogether on iOS and Android devices. These steps may be sufficient for users who voluntarily choose to run ABTraceTogether on their personal smartphones. Individuals are not subject to Alberta's privacy laws, and have no legal obligations to safeguard their own personal information.

- The risk mitigation that AH has put in place (i.e. public information for users with directions to reduce risk) is not sufficient with respect to employees who may be running ABTraceTogether on enterprise-issued devices (i.e. issued by regulated public bodies, custodians or private sector organizations) that store or make other health or personal information accessible.

  That is, public bodies, custodians and private sector organizations have legal obligations under Alberta's FOIP Act, HIA and *Personal Information Protection Act*, respectively, to make reasonable security arrangements to protect health and personal information in their custody or control. The risks represent a potential contravention of Alberta's privacy laws by regulated entities if they were to allow employees or affiliates to run the app on enterprise-issued devices that store or make other health or personal information accessible.

Summary of Recommendations

[263] We made the following recommendations during our PIA review of ABTraceTogether:

Notice

- AH review the description of the app available from the Google Play Store and Apple App Store to ensure it accurately describes the app.
- AH review and confirm its authority to collect, use and disclose health and personal information under HIA and the FOIP Act, as well as the purposes for which it collects, uses and discloses this information, and update the PIA, privacy notice, FAQ and privacy policy accordingly.
- AH review public materials describing the app's functionality to ensure that it is clear that the app logs all "handshakes", and the purpose for doing so.

Consent

- AH review the wording of the consent against the requirements set out in both HIA and the FOIP Act to ensure the requirements are met and to avoid confusion.

Limited Collection, Use and Disclosure

- AH work towards limiting collection of "handshakes" through any means available to them, to be transparent to the public regarding potential over collection, and to update the PIA, as necessary, if changes are introduced.

Data Matching

- AH provide additional information to clarify its position. If data matching is taking place, AH is required (by Part 6, Division 2: Data Matching of HIA) to explain how risks are mitigated.

Organizational Privacy Management

- AHS address any outstanding issues with its Organization Privacy Management PIA.

Project Specific Policies and Procedures

- AH review its policies, particularly concerning access to and use of data in the analytics environment, as well as the legal authorities cited in the PIA's legal authority table, to ensure consistency.

Risk Assessment (PIA Compliance)

- AH address recommendations made in this report and update its PIA as appropriate, and include AHS in monitoring and reviewing ABTraceTogether such that PIA amendments can be submitted by both custodians in a timely manner.

- AH publish PIA revisions and information concerning compliance with recommendations made in this report, as well as information about the use of the app (e.g. take-up by Albertans) and its effectiveness in meeting stated goals and objectives.

Training for Contract Tracers and Analytics Staff

- AH clarify how AH and AHS ensure that the ABTraceTogether training is completed and tracked and whether all AH and AHS users of ABTraceTogether are provided access to and training on the four policies provided during the PIA review.
- AH publicly communicate the risk that an individual might be able to infer who exposed them to COVID-19 if they are strictly limiting contact with others, so individuals can consider this risk before downloading and using the app.

Security in Contracting with Third Parties

- AH confirm when its change order with IBM has been finalized.
- AH provide additional information to confirm that the agreement meets requirements set out in section 66 of HIA and sections 7.2 and 8(4) of the HIA Regulation, with respect to the services Twilio provides.

Securing Data in Transit and Data at Rest

- AH consider further obfuscating user IDs through the use of "salting".
- AH implement encryption for data at rest, especially for the operational database that stores user ID and phone number pairings.

Monitoring and Auditing

- AH provide an update on its audit strategy after implementing the strategy.

Withdrawal from Participation and Off-Boarding

- AH review its public documents to ensure they are clear that only the phone number is deleted when a user withdraws participation, not the user ID.

Retention of Personal and Health Information

- AH provide information concerning the retention of information used to contact someone who has potentially been exposed, and where that information is recorded and for how long it is retained.

Decommissioning ABTraceTogether

- AH engage with the OIPC when it is time to dismantle the application, and provide an update on its decommissioning plans publicly.

Functionality

- AH continue to make information available to users concerning how the functionality issues contribute to privacy risks for individuals.
- Individuals review the materials AH has made public as well as other resources, so that they can make an informed choice to run the app with full knowledge of potential risks to privacy.
- AH continue to make available the ABTraceTogether source code, and to commit publicly to publishing updated versions of the source code.
- AH continue to liaise with the necessary parties to arrive at a solution for the security limitations, and to submit a PIA amendment should such changes occur.

Christine Wagoner and Eric Cheung
Senior Information and Privacy Managers