ABTraceTogether Privacy Impact Assessment Summary

Purpose

The purpose of this Privacy Impact Assessment (PIA) is to provide the Office of the Information and Privacy Commissioner (OIPC) with a refreshed PIA that describes the current state of the ABTraceTogether application as of the submission date. The PIA describes updates and changes that were made: to improve the reliability and effectiveness of contact tracing, to address the previous OIPC privacy and security recommendations, and to implement functionality changes to encourage adoption of ABTraceTogether by Albertans.

About ABTraceTogether and Contact Tracing Apps

The development and implementation of ABTraceTogether, a mobile application ("App"), is one way Albertans and public health professionals can work together to limit the spread of COVID19. As an integrated public health tool, the ABTraceTogether App complements manual contact tracing efforts and equips public health contact tracers to understand the nature of the spread of COVID-19.

Contact tracing applications work by exchanging anonymous randomly generated IDs with other smartphones running the application, in an effort to exchange and log close contacts between individuals who may have encountered someone who has contracted COVID-19. Users voluntarily download the App, register with their mobile phone number, and activate Bluetooth. Smartphones with the App enabled can communicate with each other over Bluetooth by sharing randomly generated IDs. Individuals who test positive for COVID-19 are asked to voluntarily upload this encounter data gathered by the App. Public health officials can then trace potential close contacts of the individual with COVID-19 to curb COVID-19 transmission.

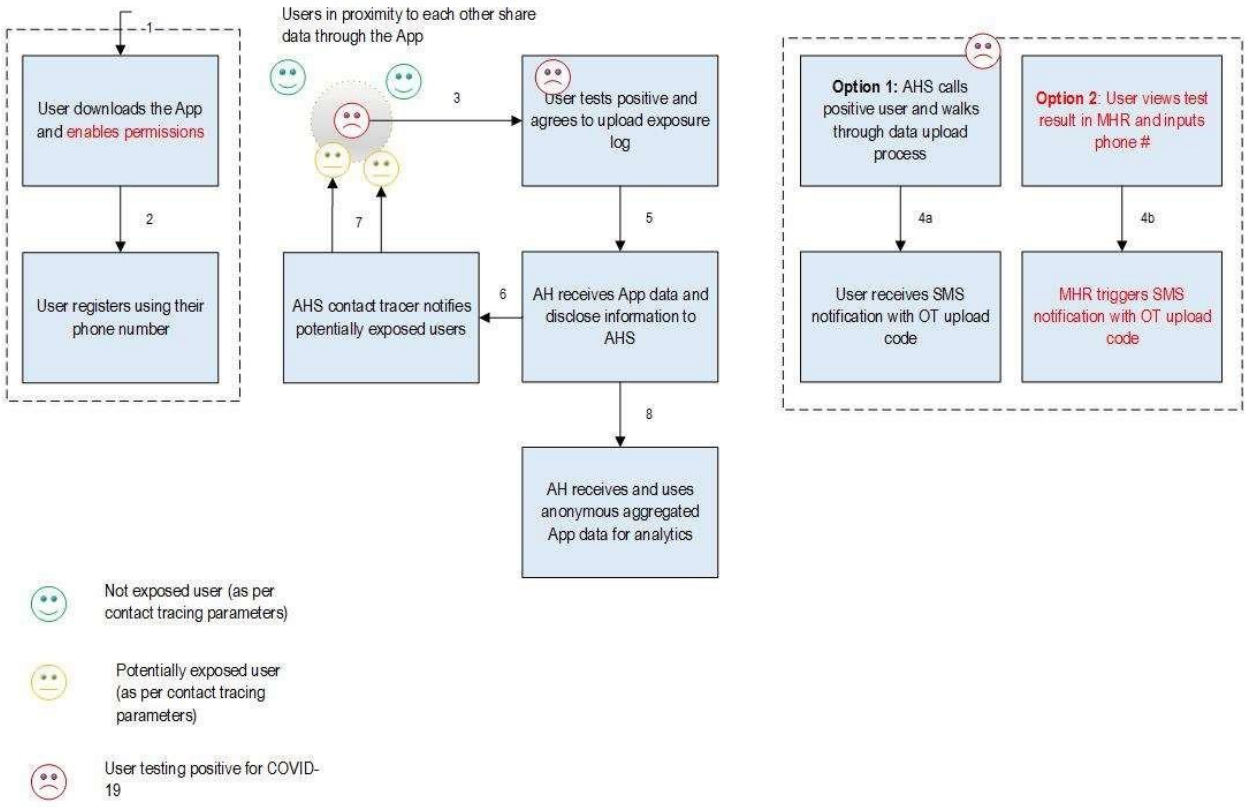
Alberta Health developed ABTraceTogether with both the information needs of Alberta's public health response and the privacy of Albertans in mind. ABTraceTogether also provides information on COVID-19 statistics and public health guidance. Updates to the App were made to improve its contact tracing and background performance while providing adequate epidemiological data for use in preventing the spread of COVID-19.

The App will only be used for the duration of the province's response to the COVID-19 pandemic. Once the pandemic is over, the App will no longer be available for download, and the program will be dismantled.

ABTraceTogether is available for download on iOS and Android devices. When registering, users are presented with a collection notice and asked to consent to the use of the information collected through the App. Users can opt out at any time. Please see Appendix A for the ABTraceTogether in-app Privacy Statement Summary and the ABTraceTogether website for the full Privacy Statement.

ABTraceTogether is Designed to Protect Privacy

The following diagram shows how the App works and how data will be collected and used by Alberta Health and Alberta Health Services (AHS).



ABTraceTogether protects user privacy through key privacy features, including:

- Limited information is collected by the app,
- Location information is not collected by the app
- Users choose if they want to upload their data, and
- Users can opt out at any time.

Limited Information Collected

ABTraceTogether collects limited data. During registration, a user's mobile phone number is collected and paired with a User ID. Contact tracers use this number to contact individuals if they are later identified as being a potential close contact of a COVID-positive user. Mobile numbers are never revealed to other App users.

Location is Not Tracked

ABTraceTogether only collects and sends anonymous data between App users who are in close proximity to each other. Users must enable both Bluetooth and Location Permissions. However, enabling Bluetooth and Location Services is used solely to improve the App's functionality by allowing the App to operate regardless of the device's lock/unlock state or the App's foreground/background status. Personal information, and location information or GPS coordinates are never used, captured, or stored.

Bluetooth-enabled encrypted IDs are shared between user devices when there is a potential for exposure based on the length of time users have been in close proximity, creating a log of potential exposures. Exposure logs are not used to identify where users have been.

The anonymized data that is collected and stored by the App will be automatically deleted from a user's phone after 21 days. The action of deleting the App will remove the App and its data from the phone.

Users Control Upload

ABTraceTogether is voluntary; users may choose not to upload their App data. If a user tests positive for COVID-19 they can voluntarily upload their information to assist with contact tracing efforts. If they choose to share their information, users will receive a one-time upload code to enter into their app via SMS if they identify as an app user during a phone call with an AHS contact tracer or through MyHealth Records.

The data that is shared with AHS includes the User ID and phone number provided at registration, the anonymous IDs of other users, and information about how close the positive case and other users came to each other. AHS contact tracers will use this information to contact other users (without knowing their name) who may have encountered an App user who tested positive for COVID-19.

Revoking Consent

Users can revoke their consent by deleting the app from their phone and emailing hiahelpdesk@gov.ab.ca with the mobile number used to register the App. The user's mobile number will then be deleted from Alberta Health's server. All data that the user's phone has exchanged with other phones is rendered meaningless as it will no longer be associated with the user.

For more information about how ABTraceTogether works, please see ABTraceTogether's FAQ. The FAQ is a living document updated as needed to address questions concerning the ABTraceTogether application, and is available online from https://www.alberta.ca/ab-trace-together-faq.aspx.

Data Analytics

Data analytics of anonymized information will facilitate the coordination of Alberta's ongoing public health response to the pandemic and help Alberta Health determine how effective the App is and to what extent the App may need to be updated or modified.

Anonymized analytics information may be used by Alberta Health to improve App performance and enhance user experience. The information used does not include contact information or data that is identifiable to a specific person or location, for example: the numbers of users, close contacts and unique close contacts, contacts notified, responses received, symptomatic cases identified, and the duration of contacts between App users. Only Alberta Health staff with appropriate permissions and training have access to these data.

App Development and Contracts

Alberta Health has contracted with Deloitte and VMware for App development, and with IBM for data storage and protection.

Deloitte will only have access to App data during the development stage. IBM has access to data on the back-end to support ongoing operation of the App. VMware has been contracted for design and development of the Bluetooth protocol used in the App and has no access to personal or health information collected by the App.

The contracts with the vendors emphasize that they must keep all application data confidential. Contractors must also ensure that reasonable security arrangements are in place to protect data from unauthorized access, use, disclosure, loss or destruction. Contractors are obligated to abide by the Alberta's privacy legislation, including the Health Information Act (HIA) and the Freedom of Information and Protection of Privacy Act (FOIP).

ABTraceTogether PIA and OIPC Recommendations

Alberta Health developed ABTraceTogether while ensuring the collection, use and disclosure of health and personal information was conducted in accordance with HIA and FOIP. As required by the HIA, a PIA outlining App functionality and privacy protection features has been submitted and has been accepted by the OIPC.

Alberta Health has been working closely with the OIPC throughout App development and has been making continuous efforts to address recommendations issued by the OIPC. Alberta Health has made changes to the App for version 2 to improve the reliability and effectiveness of contact tracing, increase access to COVID-19-related information relevant to Albertans, and address previous OIPC privacy and security recommendations.

Alberta Health reviewed and, in the majority of cases, implemented the OIPC's recommendations in the refreshed PIA, including:

- Updated public-facing documents (App descriptions in Google and Apple App stores, FAQ, and the Privacy Statement) to improve descriptions of the App's functionality, information retention, and provide transparency to App users around privacy risks (such as risk of others being able to infer who exposed them to COVID-19).
- Provided additional information on how agreements with vendors involved in App development and maintenance meet the requirements of the HIA and HIA Regulation has been provided to the OIPC.
- Implemented ABTraceTogether-specific policies limiting access to ABTraceTogether information for data analytics and secondary use purposes. All Alberta Health and AHS users that have access to data collected by the App complete training and are provided access to these policies.
- Developed and implemented an audit strategy to monitor potential inappropriate access to App data.

Alberta Health has also committed to working with the OIPC to dismantle the App after the public health emergency has passed.

In addition, Alberta Health has identified and addressed a number of privacy risks and risk reduction approaches associated with the use of ABTraceTogether:

1. Risk that App data received by AH could be accessed and disclosed by Government of Alberta staff is reduced through the following:

- Internal training, including FOIP and HIA training.
- Role-based security user groups enforce separation of duties.
- Audit logs for App data access via the Contact Tracer Web Application or database administration.
- Alberta Government staff are required to sign a Confidentiality Agreement or a contract when their employment begins.
- Staff must adhere to legislation, standards, policies and information management requirements of the Alberta Government.

2. Risk that App data could be maliciously accessed or intercepted while it is stored on a user's smartphone, or in the process of downloading or uploading data is reduced through the following:

- The App relies on anonymized IDs, and transmission of phone numbers is encrypted. Only AH staff will be able to decrypt transmitted data.
- Data on local device is encrypted and non-identifiable through the App's use of temporary IDs. Crash logs do not collect or submit identifiable information.
- Requirement for recent operating systems reduces Bluetooth vulnerability.

3. Risk that App information could be used for unauthorized or secondary purposes that users were not notified of and did not consent to is reduced through the following:

- AH has a secondary use policy in place that prohibits unauthorized or secondary uses of data.
- Contractors and administrators (including contact tracers) who have access to App data are strictly prohibited from unauthorized or secondary uses of data.

- Staff must adhere to legislation, standards, policies and information management requirements of the Alberta Government

4. Risk of corruption of data before or during transfer of data between users, or between users and AH is reduced through the following:
- The data being transferred between users is in expected format limited to renewing anonymized IDs. Data transferred from users to AH require confirmation via one time SMS code and is limited to anonymized IDs and phone numbers.

5. Risk that App data stored by AH could be lost or destroyed before users are notified of a potential contact with a positive case is reduced through the following:
- In-bound app data will be continually monitored and analyzed by contact tracers; given the seriousness of the pandemic, contact tracers will respond immediately to all potential positive cases identified through the App.
- Back-end controls protecting data including backups.
- Security assessments, vulnerability testing, and penetration testing were completed resulting in risks with potential significant impact being resolved in advance of production, while less significant risks were monitored and moved to resolution after initial rollout. Issues identified with medium or higher risks were reviewed and mitigated in advance of production deployment; remaining low risks will be monitored.

6. Risk that AH incorrectly records phone number of user or incorrectly matches phone number to user resulting in sending out incorrect contact warning information is reduced through the following:
- Anonymized IDs link users to phone numbers.
- Users are only contacted by contact tracers after a potential contact has been verified.

7. Risk that use on more than one device may result in inaccuracies with tracing
- The follow-up questions by the contact tracer will address this scenario.

8. Risk from denial-of-service attacks targeting the back-end infrastructure or risk of exploit of Bluetooth functionality is reduced through the following
- AH policies and procedures have been developed to limit the risk of attacks
- The solution was designed with denial of service protections.

9. Risk that App contractors could use or disclose personal information collected by AH through the app is reduced through the following:
- Contractors strictly limit access to and use of data.

10. Risk that phone numbers of App users may be inappropriately used or provisioned by wireless service providers is reduced through the following:
- This risk is low and exists for any activity that collects phone numbers.

11. Risk from privacy misunderstanding relating to app functionality and operations
- The App Privacy Statement, privacy notice, and frequently asked questions address the use of phone numbers, and the use of anonymized identifiers to connect with other users via Bluetooth.

The App does not collect names or location information. In the event of a positive contact, and following privacy by-design principles, the user will be asked if they would like to identify themselves to support contact-tracing efforts.

- The PIA Summary will also published to help Albertans understand how the App protects privacy while collecting limited information.

12. Risk from Android and iOS devices requiring location permission; Android/Google requiring App requesting access to Bluetooth also obtain location permissions; is reduced through the following:

- The FAQ acknowledges this requirement and clarifies that the App does not capture or use information about a user's location. The FAQ also states that location data is not collected by AH or AHS and is never sent from a user's phone to another organization for any purpose.

13. Risk that individuals might be able to infer who exposed them to COVID-19 if they are strictly limiting contact with others

- The public FAQ and Privacy Statement include language to reflect this risk.

14. Risk from user inputting another individual's phone number in MHR, triggering spam/unwanted text messages is reduced through the following:

- The App asks user to confirm the phone number they enter.

15. Risk that the App gathers information after its no longer required for pandemic response.

- AH has developed an App decommissioning plan to dismantle the infrastructure and delete collected data.