CORONAVIRUS CONTACT APP FAQS

This Q&A provides details about the coronavirus contact app that has been developed to support our health response to the virus. The app has been created solely as a public health initiative and will allow state and territory health officials to automate and improve what is already done manually.

Why does Australia need a contact app?

- The app will help keep you, your family and your community safe from further spread of coronavirus through early notification of possible exposure.
- It will be one of the tools we will use to help protect the health of the community by quickly alerting people who may be at risk of having contact with the virus.
- Use of the app will help us to move more quickly to reduce restrictions than would otherwise be possible.

What will the app do?

- The contact app will allow health officials to tell you if you have come into close contact with someone who is diagnosed with COVID-19 (coronavirus).
- If you become infected with coronavirus, the app will assist health officials to notify people you have been in close contact with so they can self-quarantine and get tested.
- This will speed up current manual processes and make it quicker to stop the spread of the virus, particularly if restrictions are eased.
- The app operates on a person's phone as they go about their day.
- It securely logs the encrypted reference codes of devices of other people who are using the app who have been in close proximity to you.
- The close contact information can only be accessed by relevant health officials if there has been a positive case to help alert those who may need to be tested.
- The app will never track your location.

Why should I use the contact app?

- Receiving early notification that you may have been exposed to coronavirus means you can be tested or go into quarantine so your health and others' is protected.
- Without the assistance of technology, finding people who may have been exposed to the virus relies on people being able to recall who they have been around and knowing the details of every individual they have been in close contact with. In many cases, we don't know the names and contact details of those we've been in close contact with (for example, at the supermarket or on the train).
- The contact app uses technology to make this process faster and more accurate.
- The contact app has been developed to ensure your information and privacy is strictly protected.

Do I have to use the contact app?

- No. Its use is entirely voluntary, but using it will help save lives.
- For the App to work, it must be running in the background on your phone. Other apps can be used at the same time.

- <u>You can delete the app from your phone at any time</u>. This will delete all the app information from your phone.
- At the end of the Australian pandemic, users will be prompted to delete the app from their phone. This will delete all app information on a person's phone. The information contained on the highly secure information storage system will also be destroyed at the end of the pandemic.

How will the contact app work?

- A user voluntarily downloads the app from the app store. The user registers to use the app by entering a name, phone number and postcode, and selecting their age range. They will receive a confirmation SMS text message to complete the installation of the app. On the basis of this information, an encrypted reference code is generated for the app on that phone. That code is changed every 2 hours to make it even more secure.
- The app uses Bluetooth to look for other devices that have the app installed. It takes a note when that occurs, securely logging the other users' encrypted reference code. The date and time, distance and duration of the contact are generated on the user's phone and also recorded. <u>The location is not recorded</u>.
- This information is securely encrypted and stored on the phone.
- The app uses a rolling 21 day window to allow for the maximum 14 day incubation period, and the time taken to confirm a positive test result. The rolling 21 day window allows the app to continuously note only those user contacts that occur during the coronavirus incubation window. Contacts that occurred outside of the 21 day window are automatically deleted from the user's phone.
- The contact information on the phone is not accessible by anyone (including the user of the phone), until the user is diagnosed with coronavirus and they upload the contact information to a highly secure information storage system.
- The uploaded information enables state or territory health officials to contact the user and close contacts to provide advice on actions they should take to manage their health.
- This cycle continues if a user of the app who was a close contact subsequently tests positive.

If a user receives a close contact notification, will they be advised who the contact was?

- No. This will operate in the same way as existing contact processes run by State and Territory health officials.
- A phone call will be made to users who have had close contact with another user once that user is independently confirmed as having COVID-19. This phone call will be made by State or Territory health officials.
- Close contact information is only available to State and Territory health officials once a user is confirmed as coronavirus positive, and the user securely uploads the information stored on their phone.
- These calls will only be made to close contacts that have occurred in the 21 days before the information has been uploaded. This early notification allows users to quickly self-quarantine and seek medical attention.

Who is a "close contact" for notification purposes?

- State and Territory public health officials will have the contact information for other users who have been within approximately 1.5 metres of the infected user for 15 minutes or more.

How does the app know a "close contact" has occurred?

- When two (or more) app users come into close proximity their phones exchange Bluetooth signals and make a series of 'digital handshakes'.
- The app records the encrypted reference code, time and proximity of two users, through the strength of the Bluetooth signals. This allows the approximate distance between the users and the duration the contact occurred to be determined once the data is uploaded to the highly secure information storage system.
- The proximity for a close contact is approximately 1.5 metres, for a period of 15 minutes or more.
- To be effective, users should have the app running in the background of their phone whenever they are coming into contact with people. Users of the app will receive daily notifications to ensure the app is running.

Why does the app only notify close contacts in the last 21 days?

- The average incubation period for someone who contracts COVID-19 is typically 5 to 6 days, however the World Health Organization currently estimate that the incubation period can be up to 14 days.
- The app uses a rolling 21 day window to allow for the maximum 14 day incubation period, and the time taken to confirm a positive test result.
- The rolling 21 day window allows the app to continuously monitor only those user contacts that occur during the coronavirus incubation window.
- Contacts that occurred outside of the 21 day window are automatically deleted from the user's phone.

Is there a risk that people may report false positives?

- Information collected by the app that is uploaded to the highly secure information storage system will only be accessed by state and territory health officials once a user has a positive diagnosis. This positive diagnosis must be verified by health officials.

What information is captured by the contact app?

- The app only uses the information that's needed to alert close contacts and allow health officials to make contact with them.
- This information is only the encrypted reference code, date, time, duration and proximity of contacts.
- At registration, the user provides their name, phone number and postcode, and selects their age range, which generates an encrypted code
- All further information about contacts collected by the app is encrypted and stored within the app on the phone. Users cannot access contact information stored on their phone.
- If the user deletes the app, all contact information is deleted.
- The contact information on the phone is not accessible by anyone, unless the user is diagnosed with coronavirus and they upload the contact information to a highly secure information storage system.

Can the app be used to track a user or contact?

- No. It does not record an individual's location or movements. The app only records that a contact occurred to allow health officials to contact those users to enable them to quickly self-quarantine and/or seek medical attention.
- The app cannot be used to enforce quarantine or isolation restrictions or any other laws.
- Commonwealth and state/territory law enforcement agencies will not be allowed to access any information from the app, unless investigating misuse of that information itself.

Why does the app ask for your mobile phone number?

- A mobile number is needed to activate an account and to allow health officials to contact you if they need to.

Can a user or health official view the information stored on the phone including the contact log?

- No. All information that is stored on the phone is digitally encrypted and cannot be accessed or viewed by any users or health officials.
- Contact information older than 21 days on your phone is automatically deleted.

How will the information be stored?

- When a person registers the app, a name, verified mobile number, age range and postcode are registered and encrypted on the highly secure information storage system. They are provided an encrypted hash code, which is the only data shared as part of the Bluetooth 'digital handshake'.
- The digital handshakes collected by the contact app are stored locally on the user's phone.
- Contact information only leaves the users phone if the user is diagnosed as having coronavirus.
- Contacts that are older than 21 days are automatically deleted from the phone.
- The information is uploaded to a highly secure information storage system. Only authorised state and territory health officials will have access to the contact information. State and territory health officials will only have access to view the contact information collected by people from their state or territory diagnosed with COVID-19.
- In accessing and using the uploaded data, health officials will be required to comply with the Australian Privacy Principles and all applicable data protection and information security obligations. It will only be able to be used for alerting individuals if they have come into contact with a person who has contracted coronavirus.

How does this new app relate to the Australian Government Coronavirus App and WhatsApp service?

- The app is a separate, new app. Its sole purpose is to improve the ability of health officials to quickly alert and contain virus outbreaks in the community.
- The Australian Government Coronavirus App and WhatsApp services are information services. They were developed to ensure the community has access to timely and accurate information about coronavirus.

How does the contact app relate to other contact apps that have been released?

- This app is the only contact app that has been developed by the Australian Government Department of Health to ensure your data and privacy are protected.

- Other contact apps do not have the support of the Australian Government.

How is my privacy going to be protected?

- The Health Minister has issued a Determination under the Biosecurity Act to protect people's privacy and restrict access to app data to state and territory health authorities for contact tracing.
- It will be a criminal offence to use any app data in any other way.
- Other agencies, including law enforcement, will not be able to access the information unless investigating misuse of that information itself.
- These provisions will be enshrined in legislation when Parliament returns in May.
- The app also has a range of privacy and security safeguards built in, including no collection of geolocation data and secure encryption.
- An independently developed Privacy Impact Assessment detailing the App's compliance with the Privacy Act and Australian Privacy Principles has been made publicly available.

Will legislation be required for the app to operate, or for individuals' privacy to be protected?

- No. Use of the app is voluntary.
- Collection and use of information from the app is consent based and consistent with the Privacy Act and Australian Privacy Principles.
- To further strengthen the app's privacy arrangements the Health Minister made a Determination under the Biosecurity Act to protect people's privacy and restrict access to app data to state and territory health authorities for contact tracing.
- Under that Determination, it will be a criminal offence to use any app data in any other way. It will also be a criminal offence for someone to be refused to enter a premises, participate in an event or receive a service for failing to use the app.
- These provisions will also be enshrined in legislation when Parliament returns in May.

What information is being collected and what is not being collected?

- Information collected includes registration information, contact information and app logs:
    - Information collected at registration includes name, mobile number, age range and post code;
    - Contact information includes encrypted reference code, date and time, proximity and duration of contact; and,
    - App logs include app performance and troubleshooting data, including errors if any.
- The app does not collect any other additional information, such as location information, movement information etc.

What consequences are there if a person using the app tests positive for COVID-19 but then refuses to provide consent to upload their data?

- As is currently the case, people that test positive for COVID-19 will be required by state or territory health officials to provide their contact information.
- The app is a more efficient and faster way of doing that, and can provide additional information of contacts that they may not know, such as the person standing next to them at the supermarket.
- Whether or not they use the app information, they will still have to go through the current process of recalling all their recent contacts and providing that to their state or territory health officials. The app adds to this process and makes it quicker.

Technical Aspects:

- The app will perform digital handshakes with all other contact apps in Bluetooth range.
- The app records Bluetooth signal strength to allow approximation of distance.
- The app will poll every minute for new connections and to record the duration of existing connections.
- This digital handshake information, which does not include any identifiable data, is all recorded on the phone. It is uploaded to the highly secure information storage system when consent is given by a positively diagnosed user.
- A filtering process on the highly secure information storage system separates information that meets the close contact requirements and makes it available to the relevant state and territory health officials.