Data Privacy Notice “COVID Trace” App

1. Introduction

The purpose of this privacy notice is to explain how the COVID Trace App (the ‘app’) works, what data is collected by the app, who has access to that data and the purposes for which the data is used.

The app is available to download for free from the Apple App Store and the Google Play Store. Use of the app by you is completely voluntary – it is your choice to download it, your choice to keep it on your device, your choice to use the different services that are available on the app, and your choice to delete it. You can choose to delete any data saved by the app and/or delete the app at any time.

2. What the app does

The app helps support the overall national public health response to the coronavirus (COVID-19) pandemic by assisting members of the public through the following functions.

- Exposure Notification – to attempt to notify you as quickly as possible should you have been in close and sustained contact with someone who has tested positive to COVID-19.
- News and Information – to attempt to give you convenient facts and figures about COVID-19 in Nevada.
- Other Functions – the app can collect metric data (see section 3.3) that is based upon metrics and will remain anonymous which is used only by the State of Nevada and the Department of Health and Human Services (”DHHS”) public health teams to assist in monitoring how the app is contributing to the response efforts and get a better understanding of the spread of the virus. It is important to know that removing the app from your phone will delete all data collected. .

3. About the COVID Trace App

3.1 How Exposure Notification works

Existing manual contact tracing processes (i.e. collecting information directly from people about phone or in person contact) rely on people being able to remember who they have been in contact with recently, and how long that contact lasted. In many cases people do not know the identity of other people they have been in contact with (for example, if the contact occurred on a bus or train, at a concert, a restaurant or some other public venue).

The app uses technology developed by Apple and Google called COVID-19 Exposure Alerts where anonymous rolling identifiers are exchanged within Bluetooth range of about 300 feet. that have the app installed. Exposure Alerts enable your phone to generate a random, unique key every 10 to 20 minutes. Remember, the key is anonymous. If you are close to another phone that also has Exposure Alerts turned on, both apps work together to exchange anonymous keys, retaining the anonymous information in the keys on each phone. Again, while the information in the keys mutually remain on the phones, the keys cannot identify either person to anyone else, DHHS or the State of Nevada.

However, if you subsequently receive a positive COVID-19 diagnosis, you will receive a call (not a text) from the Contact Tracing Center ('CTC') within the State of Nevada to inquire if you have been using the Contact Tracing feature on the app. If you are using the feature and you choose to do so, you can upload the keys on our phone to a State of Nevada Registry which will assist DHHS in the contract tracing process. The keys and their anonymous information are published to assist the public. At this stage, the keys are known as Diagnosis Keys.

Every two (Android) to four (iPhone) hours, the latest Diagnosis Keys from the State of Nevada Registry will be downloaded by the participating user's app. The app on each participating user's phone will check for matches against the keys that have been collected by each user's phone. If there is a match indicating that a user sustained close contact with a person who was diagnosed with COVID-19, the app will notify the user. This is called a 'Potential Exposure Alert'. Remember, the notification is within the app, there will never be a separate text message for this notification.

For all this to work, each user must turn on the Apple/Google Exposure Alerts service on their phone. Each user will be presented with an option to allow the app to use this service and to turn this service on during the initial screens after the app has been installed. Each user can change their mind about using the app at any time by turning the service on or off at through the app settings.

If a user receives a Potential Exposure Alert, a message will display prominently within the app. Again, the alert will never be sent by text. However, each user can also choose to allow the app to display a phone notification in the event of a Potential Exposure Alert. User's who desire to have a phone notification may agree to do so by choosing to allow Alerts option selected during the initial screens after the app has been installed. This option can be changed at any time through the app settings.

As an option in the event a user receives a Potential Exposure Alert, each user who wishes to speak to someone at the department of health may do so by initiating a call to the Department of Health hotline from within the app.

Again, it is important to know that neither the app nor the service reveals the identity of any person using the app to other app users, the State of Nevada, or anyone else. In addition, neither the app nor the service reveals the identity of any user that has been diagnosed positive or negative with COVID-19. The State of Nevada will not know if you received a Potential Exposure Alert.

3.2 What News and Information is

The app will provide users with the latest updates about coronavirus (COVID-19) in State of Nevada. While this information is already available on https://nvhealthresponse.nv.gov, the app provides an alternative way of viewing the keys. The information that can be viewed includes statistics such as the total number of confirmed cases, number of deaths, numbers hospitalized, and the number of cases per county in the State of Nevada.

3.3 What app metrics are collected

Metrics collected and sent to the State of Nevada are utilized by DHHS and public health teams to understand user use of the apps, the app effectiveness as part of the pandemic response, and provide information to improve the app and its effectiveness in contract tracing of COVID-19. Remember, Metric data does not identify users and is used to create aggregate views of the apps use and the impact on mitigating the spread of the virus. Only with user consent, the following metrics are collected from the app.

- Whether the app on a user's phone and in use
- Whether the app completed setup
- Whether the app has received a Potential Exposure Alert
- Whether the app has uploaded diagnosis keys
- The number of diagnosis key matches per Potential Exposure Alert
- Number of days between the app triggering a Potential Exposure Alert and the upload of diagnosis keys, if applicable
- Whether a call was initiated to the Department of Health from the app

4. What data is collected and processed

Again, the information processed by the app is anonymous.

This information is processed in 2 different ways, depending whether the information has been provided by:

- the Exposure Alert service;
- the user's phone through the app.

4.1 The Exposure Alerts service

The Contact Tracing function works by enabling the Exposure Alert Service in the app. The following data is processed for the operation of Exposure Alerts service if enabled:

. Keys sent and received between phones that have the service turned on.

. Diagnosis keys uploaded to the State of Nevada Registry if the user is COVID-19 positive and agrees to upload them.

. Diagnosis keys downloaded from the State of Nevada Registry to all apps for matching.

The above keys are pseudo-random alpha numeric values that cannot be used to identify any user. These are generated, collected and matched on a user's phone only if the user enabled the Exposure Alerts service.

4.2 Provided by your phone or the app

As a consequence of how network traffic passes across the Internet, user's Internet Protocol (IP) address is also inevitably transferred to State of Nevada servers. An IP address is typically made up of 4 sets of numbers (e.g. 1.2.3.4) and is assigned to each user by the user's mobile phone or Wi-Fi service provider. Under the data protection law each user's IP address is generally regarded as personal data.

During the initial screens following installation, the app carries out tests to verify if the app is a valid State of Nevada app and the phone is a real device. Upon confirmation, the app connects to the State of Nevada servers and exchanges security tokens to protect the app from security attacks. The security tokens are not used to identify users and are only utilized to verify that Internet traffic coming from the app while installed and running is from a confirmed COVID Tracker App running on an actual phone.

While user data transmitted between the app and the State of Nevada servers includes the IP address, the State of Nevada does not use user IP addresses to identify users. User's IP addresses are removed by the State of Nevada servers upon the apps contact with the servers and stored without identification to prevent abuse. The IP address information is stripped from the keys and cannot be associated to the user.

The Metric data is collected by the app and is shared with the State of Nevada as described previously.

5. You Consent to the Collection of the Described Data

Use of the app is voluntary. Use of the App means that a user consents to the collection and use of the data collected through keys described above. Consent is revoked by the user deleting the app which will delete any key data.

6. Security measures

All data stored by the app on a user's phone is encrypted using the built-in encryption capability of each user's phone. Data is also encrypted when it is uploaded to State of Nevada servers.

The Contact Tracing feature uses a fully 'decentralized' privacy model. This means that key and diagnosis key matches are made locally on user's phones. Matches are not made externally by the State of Nevada. This ensures there is no tracking of users' movements or contacts.

There are a range of security processes and technologies in place to prevent unauthorized access to the data while it is stored on State of Nevada servers, including data encryption, modern firewalls and intrusion prevention.

7. Who processes your data

The State of Nevada is responsible for running the app and all infrastructure required to operate and maintain the app and backend servers.

7.1 Data Processors

There are a number of data processors who provide services to the app for the State of Nevada.

The following companies will have access to the data through the app:

> COVID Trace are the app developers who will provide technical support on the running of the app.

The following companies provide services to the State of Nevada but do not have access to the data through the app:

> Google Cloud Platform (GCP) provide cloud storage and cloud services for the data uploaded from your phone.

Contracts are in place between the State of Nevada and each of these third-party processors which set out the processors’ obligations and the State of Nevada’s obligations and rights with regard to the data that is being processed.

Apple and Google - the app can be downloaded free of charge from the Apple App Store and the Google Play Store. In this regard they are independent controllers as they process account names in order to make the app available for download. This processing activity is separate and apart from the processing of data through the app. Furthermore, although Apple and Google have developed a COVID-19 Exposure Alerts service, which is used in by the app, neither company views or obtains any data from the app or the Exposure Alerts service.

7.2 Other recipients of limited data

The State of Nevada anonymizes any app metric data that it receives from app users. This anonymized data is shared with the DHHS.

The DHHS will carry out statistical analysis on the data shared with it, which it will publish in line with its remit Department of Health, the Health Response, the State of Nevada, and to the public as appropriate.

8. How long is user data held for

Exposure Alerts service keys on user device through the Contact Tracing function:

Keys and their associated data is retained on user phones for 14 days. 14 days is considered a window of epidemiological significance that generally covers the potential for viral transmission.

Diagnosis keys in State of Nevada registry through the Contact Tracing function:

Diagnosis keys and associated information is retained for 14 days. As above, 14 days is considered a window of epidemiological significance that generally covers the potential for viral transmission.

Diagnosis keys on user devices through the Contact Tracing function:

Diagnosis keys and associated data on user devices is retained for as long as is necessary to perform a match check and upon a confirmation it is deleted.

App metrics:

This anonymous information is retained by the State of Nevada for a minimum of 7 years and is reviewed at that stage for extension or deletion depending on its health value. This data is retained for the purposes of monitoring the efficacy of the app and improving it.

9. Changes to this Data Privacy Notice

This Data Privacy Notice may modified from time to time and once modified users will receive notification that this Data Privacy Notice has been updated through the app.