Exposure Notification Privacy Policy

Version 1 • March 30, 2021

www.aphl.org

The Association of Public Health Laboratories (APHL) is a national non-profit organization, which recognizes the importance of protecting personal information and the individual's right to privacy. Thus, we are dedicated to maintaining high standards of confidentiality regarding the information provided to us.

The COVID-19 Exposure Notifications System was built by Google and Apple with your privacy and security central to the design. The Exposure Notification System does not collect any location data from user devices and does not share the identities of other users to each other, or the service providers.

APHL supports this system in its hosting of the National Key Server on the Azure Cloud and the Multi-tenant Verification Server on the Google Cloud Platform. These servers are available to all US states and territories.

NATIONAL KEY SERVER

The National Key Server provides temporary storage for Temporary Exposure Keys (TEKs) devoid of any personal information; it is not possible to use the TEK to identify an individual.

When devices communicate with the National Key Server the platform logs additional information. Server logs are required for monitoring the stability and security of the National Key Server. The following data is collected in the logs:

- Device's current public internet protocol (IP) address
- Date and time of communication
- Server response status (success or error code)
- Connection details (e.g., server URL, protocol, request method, user agent)

Server logs that contain the above information are retained for a 14-day period. In the event of a critical incident, server log retention may be increased for up to 30 days. Access to the server logs is limited to the APHL Technical and Security Team and access control policies implement the principle of least privilege and segregation of duty. Log access and other administrative activities are logged in Azure Sentinel and retained for 365 days.

MULTI-TENANT VERIFICATION SERVER

The Multi-tenant Verification Server provides temporary storage for the minimum information necessary to verify an individual's COVID-19 positive report. This includes:

- Non-identifiable verification codes, verification tokens and verification certificates
- Public Health Authority case workers' name and email address

When devices communicate with the Multi-tenant Verification Server additional information is logged. Server logs are required for monitoring the stability and security of the Multi-tenant Verification Server. The following data is collected in the logs:

- Device's current public internet protocol (IP) address (masked (unviewable) for all server operators except the required "Owners")
- Date and time of communication
- Server response status (success or error code)
- Connection details (e.g., server URL, protocol, request method, user agent)

Server logs that contain the above information are retained for a 14-day period. In the event of a critical incident, server log retention may be increased for up to 30 days. Access to the server logs is limited to the APHL Technical and Security Team and access control policies implement the principle of least privilege and segregation of duty. Administrative activities are logged in BigQuery and retained for 365 days.

CHANGES TO OUR PRIVACY STATEMENT

Subject to exposure notification system or server changes, we may amend this privacy statement from time to time. If we make changes to this statement, we will amend the revision date at the bottom of the page.

QUESTIONS?

If you have questions or concerns about this policy, please contact informatics@aphl.org. We will treat all privacy concerns seriously within a reasonable timeframe and get back to you as soon as possible.