Exposure Notifications

On-Device Venue Check-Ins

Preliminary — Subject to Modification and Extension

September 2021

v1.0

Contents

Overview

This document details how a Public Health Authority (PHA) can use On-Device Venue Check-Ins to alert users when someone reports a positive test result for COVID-19, the disease caused by the SARS-CoV-2 virus. This feature notifies other people who've been at the same indoor location at the same time as someone who reports a positive test result through an app on a phone or other device.

A PHA can include a feature in their Exposure Notifications app that allows people to Check-In at a specific venue, by scanning a Quick Response (QR) code or Near-Field Communication (NFC) device. This feature can notify people who were at the same venue around the same time as a potential exposure, even if Exposure Notifications didn't record them being near a person at the venue who reported a positive test result. This feature is not a part of Exposure Notifications and users must opt-in to use the feature in the PHA's app and separately opt-in to share their Check-In information after a positive test result.

There are two options for performing Check-Ins:

1. On-Device.

   Venue Check-Ins stay on the device. Human contact tracers identify venues where people who report positive test results have recently visited during a period when they were likely contagious. These contact tracers manually enter venue identifiers and approximate date and time when someone who tested positive was at the venue, into the PHA server. The server periodically pushes this information to the device, and the device compares the information against the local Check-Ins. If there's a match, the system warns the user they may have been exposed.

2. Off-Device.

   A device uploads cryptographically protected venue Check-Ins to the PHA server only when the user tests positive and agrees to sharing. The Check-Ins are anonymously sent off the device, and then pushed from the server to all devices for matching. If a Check-In from the server matches a Check-In on the device, the system warns the user they may have been exposed. This option doesn't need human contact tracers to input any information.

Off-Device venue Check-Ins require positive users to share their Check-In information, and remove the need for human verification; matching occurs automatically. On-Device Check-Ins stay on the device, which gives users more control over their private information.

When a user opts-in to sharing their venue Check-In information, the PHA app sends only limited data to the PHA's server, for example, a venue identifier, the approximate date and time when the user was at the venue, and a transmission risk value. It must not send any personally identifiable information about the user when it sends the Check-In information. The PHA's app cryptographically protects the data it sends to the PHA, and must not send any data to Apple or Google. Neither Apple, Google, nor the PHA have access to the protected Check-In information.

Definitions

- Check-In Mechanism — A QR Code, bar code, NFC device, or any other automated mechanism people can use with their phones to Check-In at a venue.
- Check-In — The event when a person uses the Check-In Mechanism to record on their phone the fact that they were at the venue at a specific time.
- EN — Exposure Notifications, as developed jointly by Apple and Google.
- Venue — Any event, venue, or other location that offers Check-In.

On-Device Venue Check-Ins

When a person uses the Check-In Mechanism, their phone receives and records data provided by that mechanism. The data received from the Check-In Mechanism can include information, such as a venue name, address, or a default attendance duration.

If a PHA uses an NFC device or any other device capable of two-way communication, the phone must not send any user-identifiable or device-identifiable information back to the Check-In Mechanism.

User Check-In

When a person arrives at a venue that supports the Check-In System, they can use their phone to Check-In. When they use the Check-In Mechanism, their app must securely store the date and time of the scan. During Check-In, the venue must not record any information.

Check-In data must only be stored locally on the user's device. The app must delete a check-in permanently when 14 days have passed since the Check-In. iPhone backups do not include Check-In data, and users can view all Check-In data in the app. The app must provide a way for the user to delete individual Check-Ins, as well as have an option to delete all Check-In System data.

After a Check-In, with the user's permission, their phone will periodically download data from the PHA's server so that the PHA's app can check whether the user was present at the same time as declared positive COVID-19 cases at the venue.

App Requirements

PHAs that implement the Check-In System must include additional user-facing functionality in their app.

1. The Check-In System is a separate feature from EN. Accordingly, the app must use a completely separate flow for implementing the Check-In System.
2. The app must keep Check-In data exclusively on the user's device and must not send it to any server or back it up in the app's datastore.
3. The app must store all information related to Check-In activity exclusively on-device with data protection ClassA: CompleteProtection or Class B: Protected Unless Open, except for data necessary to do on-device matching. For more information on data protection classes, see https://support.apple.com/guide/security/data-protection-overview-secf6276da8a/web
4. The app must use local notifications to inform users about potential exposure at a venue. The app must not transmit Check-In data (including associated or derived data) to a server and the app must not transmit data related to matching to a server or central authority.
5. The app must automatically and permanently delete any Check-In records and all associated and derived data once the Check-In is more than 14 days old.
6. The Check-In System must be optional. Venues cannot require people to use Check-In to gain entry to public transit, markets, or officials buildings.
7. The app must provide a visible and human-readable list of captured locations.
8. The user must be able to manually delete any or all records at any time, including all associated data on device.

Venue Requirements

1. Venues must not require attendees to Check-In using the app, or make services (such as access to public transit or buildings) contingent on a user Check-In using the app.
2. Venues must provide an alternate way to Check-In that doesn't require the use of the Check-In System feature.

Public Health Authority Requirements

1. PHAs must not attempt to profile or identify users, for example, by mapping the physical venue to the Check-In Mechanism cryptographic seed or by any other means.
2. PHAs must publicly publish a buildable copy of the source code for their EN app including any external libraries or dependencies. PHAs must update the published copy with every subsequent submission to the App Store.

Revision History

v1.0 - September 1, 2021

- Initial version.