Quarantine Agent

DXC COVID-19 Safety Suite

Table of contents

General

What is the DXC COVID-19 Safety Suite?

The DXC COVID-19 Safety Suite is a curated collection of tools to address pandemics, tailored to the characteristics of the novel coronavirus (2019-nCov acute respiratory disease) that causes the COVID-19 disease. Typically delivered as a service with optional business process outsourcing (BPO), its components include licensed partner provided, open source, and in-house hardware and software.

What is the purpose of the Quarantine Agent module?

The Quarantine Agent component of the DXC COVID-19 Safety Suite uses artificial intelligence/machine learning to create a virtual quarantine enforcement agent, freeing up human agents to investigate escalated instances. Quarantine is a key part of any effective social distancing strategy for controlling an epidemic or pandemic.

Why is social distancing necessary?

According to modelling by the University of Sydney, Social Distancing (SD) strategies offer “no benefit for lower levels of compliance (at 70% or less) — these levels do not contribute to epidemic control for any duration of the social distancing restrictions. Only when the SD compliance levels exceed 80%, there is a reduction in incidence and prevalence.”[1]

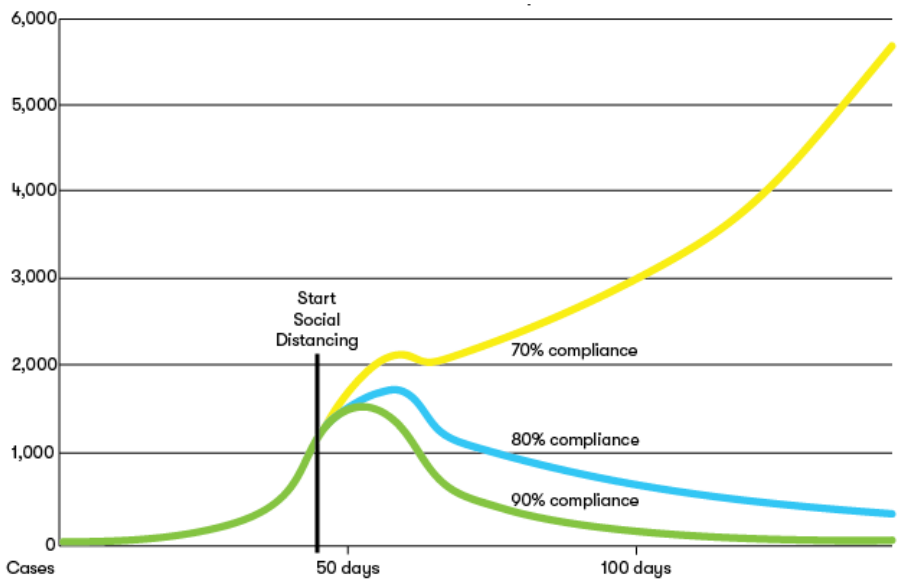

Figure 1. Quarantine compliance chart. Data source University of Sydney.

[1] Modelling transmission and control of the COVID-19 pandemic in Australia, University of Sydney.

How does Quarantine Agent work?

When participants are onboarded, typically by the authorities, they are sent a message inviting them to take a photo of themselves (“selfie”) within a specified period of time, at their chosen or allocated quarantine location (e.g. home, hotel, clinic, hospital, or dedicated facility) and incorporating a unique background. They are then periodically requested to take a new “selfie” within a short timeout period, which is compared to the baseline.

What is the audit cycle?

Participants are periodically audited for compliance with quarantine conditions via text message and web app, by taking a “selfie” which is analysed by an AI agent and escalated to a human if required.

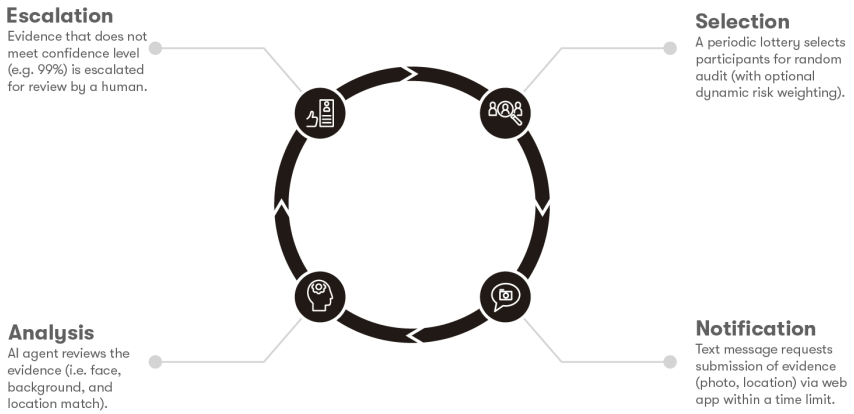

Figure 2. Quarantine Agent audit cycle.

Onboarding

How are participants onboarded?

Operators provide a mobile number via a secure web form, and the participant is immediately invited to check in for the first time.

Can operators onboard multiple/many participants at once?

Yes. Operators upload participants’ mobile numbers via a secure web form, one per line, and the participants are immediately invited to check in for the first time.

Can operators automate the onboarding of participants?

Yes. An API can be provided for onboarding participants, which can be used to integrate the service with existing systems.

What additional data can be provided?

Only a mobile number is required, in accordance with the principle of least privilege. Operators who wish to have access to additional information, for example in escalated instances, can provide additional fields (e.g. name, date of birth, passport number, national identity number). In any case, data must be “adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed”.

Selection

How are participants selected for audit?

During onboarding, participants are automatically allocated a random numeric “ticket” in the database. A lottery is run regularly (typically every 1-60 minutes) and a percentage of the ticket namespace is selected. For example, if we are auditing between 7am and midnight (17 hours), run a lottery every 10 minutes (~100 per day), and want to audit everyone on average 3 times per day, then we need to select ~3% of the ticket namespace per lottery (~300% coverage). For example, with 1,000,000 tickets, the block of numbers 100,000 through 130,000 could be selected (30,000 = 3%) and an audit agent instantiated for any participants with one of those numbers.

Is it possible to weight participants in the lottery?

Yes. In addition to the global frequency and probability of lottery selection, there is a second probability that defines whether a selection is accepted or abandoned. When this feature is used, it typically defaults to 0.5, meaning that 50% of the time, a selection in the lottery is abandoned. We can reduce this for participants who are less able to respond quickly regularly or increase it for those who need extra attention. Note that it is necessary to tune the lottery accordingly (for example, by doubling the percentage selected on the basis that only half will be accepted).

Can participants be weighted dynamically?

Yes. This feature would typically be used to back off auditing of participants with each successful audit (for example, by decrementing their probability by 0.01 each time), or conversely to increase auditing for participants who fail to check in (for example, by increasing their probability by 0.1 each time they miss or fail a check-in).

Notification

How are participants notified that they need to check in?

Short Message Service (SMS) text message, containing a unique link for that audit instance, and instructions to click on it to check in. These are sent from Amazon Web Services (AWS) via the Simple Notification Service (SNS) by default.

How long do participants have to respond?

Timeouts are configurable and should be set to give the participant enough time to respond to the message, bearing in mind they may be otherwise engaged, but not so long as to allow them to return home — the primary purpose of the system is to validate that they are at home. 2-5 minutes is recommended, but this is configurable.

What happens if they miss the first timeout?

The system will usually give the participant a second chance to respond, typically in a shorter period of time (1-3 minutes).

What happens if they do not respond in time or at all?

At this point it is generally necessary to engage a human agent, who will typically follow up by voice or video call. For high volume deployments it is recommended this process be integrated with call centre systems such that the call is automatically placed, and participant timeline retrieved automatically for the agent.

How is the sender identified?

In mobile networks that support Sender ID, an 11-character alphanumeric identifier can be used (e.g. “Quarantine”). Otherwise a number from a pool is used.

How can participants identify the sender to avoid phishing?

A short, unique, user-specific identifier can optionally be used in the Sender ID (where supported), or the message itself. If a message is received containing that identifier, then the participant can be confident that it is from a trusted source.

Can participants reply to the notification messages?

No. Currently replies to notification messages, in countries where two-way SMS is supported, are not processed.

Can I use a custom number for the SMS messages?

Yes, however it will require integration with Twilio, as custom numbers are not supported by Amazon Web Services (AWS). The benefit of using a custom number is that it will be in a familiar format for participants and can be connected to an interactive voice response (IVR) system or call centre.

How do participants respond to a notification?

Notifications contain a unique URL for that audit cycle, and participants must click on it to provide evidence that they are still under quarantine within a specified timeout period. The link will open a web browser, which may request permission to access the phone location and camera. A preview of the rear (“selfie”) camera is shown, and the user must take the photo and confirm for it to be submitted to the server for processing. Once submitted, the photo cannot be resubmitted or modified. No feedback is given to the user, other than to confirm successful submission.

Analysis

What analysis is done on the photo?

Artificial intelligence is used for analysis of submitted evidence. The most important function is to verify that the participant is present in the photo, and for this we compare the similarity of the face in the submitted photo to one previously received. The system then analyses the background to verify they are in the same quarantine location chosen for onboarding.

How should the photo be framed?

In addition to having a clear view of the face (like a passport photo), the background should be sufficiently unique and immutable as to be able to verify that each photo was taken in the same place (unlike a passport photo). Participants should try to include a number of objects like windows, plants, furniture, and fittings and fixtures (lights, air conditioners, art, etc.).

What should not be included in the photo?

Avoid anything that will not reliably be present on future audits, such as people or animals, movable items (clothes, books, toys, etc.), or which may change significantly (views, televisions, etc.).

How can operators be sure the photo is fresh?

For higher levels of assurance, participants can be provided with a word or number which is to be written down and held up in the photo. This will also undergo analysis by artificial intelligence (optical character recognition) and the system will verify that the specified phrase appears in the photo. This prevents participants from taking the photos in advance for submission by someone else. Due to the user experience impairment, this is not recommended unless required for a certain cohort.

Can the participant change quarantine location?

No, they will need to start a new quarantine to establish a new “baseline”, albeit for a shorter period. For simplicity and security, we do not allow participants to access or change information about their quarantine, only submit evidence as and when requested to do so. Operators should cancel the existing quarantine and invite the participant to start a new one for the remaining period (e.g. 4 days if they had already served 10 of a 14-day quarantine).

Escalation

How is an issue escalated from AI agent to a human agent?

Escalations are treated as “tickets” and submitted to the preferred trouble ticketing system (e.g. Atlassian Jira, ServiceNow). Information about why the incident was escalated (late or missed check-in, participant not present in photo, too far from quarantine location, etc.), as well as context for the escalation (e.g. latest photos) and a deep link into the system for the full timeline is provided.

Do customers need to provide a call centre?

No. Customers who do not have call centre infrastructure can use DXC’s Business Process Outsourcing (BPO) services to handle escalations.

Security

How is the data protected in transit and at rest?

Users are notified via Short Message Service (SMS), with a link containing a cryptographically strong unique identifier that is infeasible to guess. The URL uses the HTTPS scheme, and the server only accepts connections that use recent versions of Transport Layer Security (TLS). Once connected, the web application is retrieved and executed in the browser. Data is returned over TLS via API, where it is encrypted and stored.

What technologies are used on the client?

The web interface uses HTML, CSS, and JavaScript to collect evidence and submit it to the servers over Transport Layer Security (TLS) via an Application Programming Interface (API).

Privacy

How is this different from an app-based approach?

Participants do not need to install an application, as notifications are sent via text message and evidence collection done using the built-in web browser. The mobile operating system controls access to location and cameras, and modern browsers typically request user permissions. Once the data is submitted the web page is closed and no longer active. It will expire in due course or can be manually removed by clearing the browser cache.

Can the artificial intelligence determine their identity?

No. The artificial intelligence is used as a comparison engine only. For this reason, we do not refer to it as “face recognition”, as this typically refers to determining the identity of an individual from a photo or video. The system does not know that a photo is of a given individual, only that it matches a previously taken photo.

What happens to the data after quarantine?

Storage policies automatically securely delete data after the duration of the quarantine plus 30 days. The only exceptions to this rule are logging data generated by the system, and data exported to external systems for escalation and enforcement activities. In any case, data is “kept in a form which permits identification of data subjects for no longer than necessary”.

Hosting

How is the service delivered?

As Software-as-a-Service (SaaS).

What cloud provider hosts the infrastructure?

Amazon Web services (AWS)

Where is the infrastructure located?

Deployments are done in the federal jurisdiction of the contracting entity if there is an Amazon Web Services (AWS) region, or in the nearest region if not.

This currently includes Australia (Sydney), Ireland, France (Paris), Germany (Frankfurt), Hong Kong, India (Mumbai), Japan (Osaka & Tokyo), Middle East (Bahrain), Singapore, South America (São Paulo), South Korea (Seoul), Sweden (Stockholm), UK (London), and the United States (Ohio, North Virginia, North California, and Oregon).

Can I deploy it on my own servers?

No. The system has been designed as a cloud-native architecture in order to achieve the security and scalability goals.

Does the system use open source software?

Yes. The system uses open source components like the MIT-licensed Node.js, “an open-source, cross-platform, JavaScript runtime environment that executes JavaScript code outside of a web browser.”

Is the system available as open source software?

No, the system consists of proprietary software delivered as a service (“SaaS”).

DXC COVID-19 Safety Suite

The DXC COVID-19 Safety Suite is a curated collection of tools to address pandemics, tailored to the characteristics of the novel coronavirus (2019-nCov acute respiratory disease) that causes the COVID-19 disease.

Typily delivered as a service with optional business process outsourcing (BPO), its components include licensed partner provided, open source, and in-house hardware and software.

Learn more at www.dxc.technology

DXC Technology Singapore
1 Depot Close, #03-01
Singapore 109841
T +65.6809.9000

011-2004061. April 2020