Data Protection Impact Assessment

COVID-19 Proximity App 'StopCOVID NI'

StopCOVID NI Proximity App

The Department of Health ('DoH') in Northern Ireland proposes to introduce a mobile application called 'StopCOVID NI' as part of its 'Track Trace and Protect' project. The app, which will be entirely voluntary for the public to download and use, is intended to act in parallel, and augment the Public Health Agency's ('PHA') COVID-19 contact tracing service, assisting in breaking chains of transmission, and reducing the spread of the viral infection within the community.

The purpose of this document is to transparently assess the impact of the envisaged processing operations on the protection of personal data, and demonstrate how the rights to privacy and confidentiality of the users are appropriately protected. In light of the scale of the envisaged data processing, types of data processing, and use of new technology; the carrying out of this assessment is considered appropriate.

1. Overview

Testing and contact tracing is seen as a cornerstone of strategies employed by countries to contain the spread of the coronavirus and save lives across the globe. On the 12th May 2020 the NI Executive published the document, 'CORONAVIRUS; EXECUTIVE APPROACH TO DECISION-MAKING' outlining a 'pathway to recovery' and stating "*As context to its reviews, the Executive will take account of measures to reduce transmission, including the increased availability of testing, the use of surveillance or tracking methodology and contact tracing for those who test positive for Coronavirus or who meet an appropriate clinical case definition. Where IT solutions, such as Apps, can assist, we will use them and encourage you to do the same. However, no matter how good such Apps are, they will have limited value unless used widely across society*." [1].

Within the context of the national public-health led response to COVID-19 in Northern Ireland, the DoH is developing a mobile phone application. The app will support the Northern Ireland public health response to COVID-19 by working in parallel to the main contact tracing process already in operation by the Public Health Agency (PHA).

The app is being developed because using mobile technology can improve the current manual contact tracing process, alerting people you have been in close contact with, but don't know; with speed and accuracy. With mobile technology, we will no longer have to solely rely on a person who has COVID-19 to know and remember everyone they were in contact with. The app will allow people (using the app) in close contact with a COVID-19 case (who they don't know who has also been using the app) to be notified faster, though anonymously; to commence self-isolation, preventing onward transmission of the infection, helping us stay ahead of the virus and save lives.

2. Roles and Responsibilities

For the purposes of the app, the DoH NI is the data controller, as it is determining the means and purposes of the processing. The DoH is responsible, along with its Data Processors and Sub-Processors, for the development, testing, security, operation and maintenance of the app. The DoH is providing strategic leadership for the app, and the Department's Covid-19 Gold Digital Cell is procuring the app on behalf of the DoH, to ensure that government policies are translated into actions and implemented effectively. The DoH does not intend to collect any personal data from the app; no location data, no symptom data, and no identifying data will be processed. The app's only function is to provide a notification to 'high risk contacts' of an app user who tests positive for

[1] https://www.executiveoffice-ni.gov.uk/publications/coronavirus-executive-approach-decision-making

COVID-19. At a regional level, aggregated numbers of positive test codes input, and notifications sent will be available. None of this will be identifiable to any individual or be able to be linked (test codes to notifications). Decentralised architecture is being employed to ensure preservation of identity and maximum privacy. **The DoH is content to state definitively the any future releases of the app will not add to the stated functionality in current version being launched.**

Governance

An app Steering Committee (see 'Appendix A') has been formed to provide an external oversight and governance function, in relation to the app development, (in terms of expertise to ensure that code and system architecture complies with the ICO guidance- 'COVID-19 Contact tracing: data protection expectations on app development'). This group is tasked with, amongst other responsibilities, ensuring that the app is used for its intended purpose, data processing is appropriately bounded in time and scope, that this DPIA report is kept under review and up to date, and co-ordinating the necessary research and analysis to assess the efficacy of the app.

At the NI Assembly Committee for Health meeting 23rd July 2020 (afternoon session) a firm commitment was made by the DoH to provide regular updates to the Committee on the uptake and functioning of the app. The frequency of these reports will be agreed and updated herein. The Committee will also be circulated a copy of the DPIA prior to publication, for the purpose of scrutiny.

There are a number of data processors and other roles that are assisting the DoH in designing, building and operating the app, these are listed in 'Appendix B'.

3. Processing Overview

Use of the app will be entirely voluntary and will be available to download for free from the Apple App Store and the Google Play Store. It will run on iPhones that support iOS 13.5 (or later) and Android phones running Android 6.0 and higher. The functions of the app that fulfil the stated purposes are as follows:

3.1 Contact Tracing

The Public Health Agency (PHA) currently operates a Contact Tracing Centre to perform manual contact tracing. This is the process where a person who has been infected with COVID-19 is interviewed over the phone to identify the people they have been in close contact with recently, governed by the agreed definition of a 'high risk contact'. A 'high risk contact' is defined as having occurred where two people spend more than 15 minutes within 2 meters of each other. These close contacts are then phoned and given advice to self-isolate for 14 days, in line with public health policy, thus restricting the spread of the virus. It is important to know (from ONS survey data) that over two thirds of individuals, who test positive, have **no symptoms at the time of testing**. The process of asking the 'high risk contacts', of those who test positive, to self-isolate for 14 days, is a proven method of reducing the rate of spread of infection (stopping those with no symptoms spreading the infection onwards). The Contact Tracing functionality delivered by the app is being designed to augment the current manual contact tracing operation in Northern Ireland, not to replace it; and is proposed to work as follows:

- When a person downloads the app they are asked to enable its Contact Tracing Function. If they choose to do so the person will be asked to turn on the phone's 'Exposure Notification' Services (ENS) service. ENS is a new Bluetooth feature that Apple and Google are introducing

to support contact tracing efforts across the globe using iPhones and Android phones in a privacy preserving way.[2]

- Continuous scanning – phones with ENS active will continuously scan for other phones nearby with ENS active. When proximity is detected, the phones record this by sending each other random IDs (or in other terms anonymous 'Identifier Beacons') without the need for any user action, and include information on Bluetooth signal strengths to be used later for distance estimating.

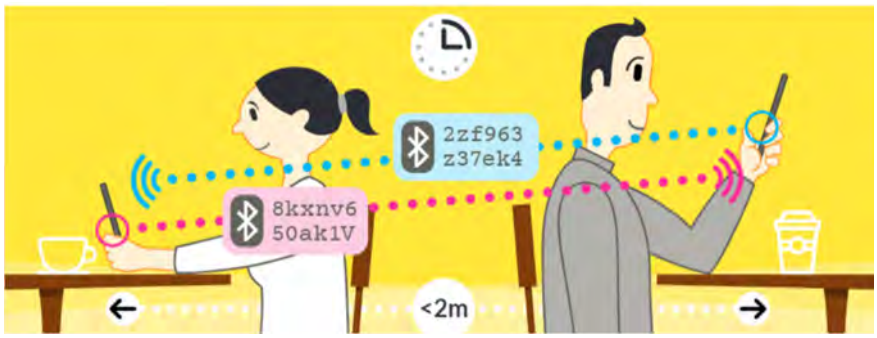


Figure 1- Phones detect each other anonymously without any user action

- A rolling 14 days' worth of theses IDs and accompanying proximity information, recording a person's recent encounters, are securely stored on the user's phone. **These IDs cannot be used to identify you**. Also, ENS, and thus Contact Tracing can be turned off and on, independent of the other app functions, at any time.

- Positive diagnosis - if a person tests positive for the virus the app user will be contacted:
  - by phone via automated SMS (where possible – where the Business Services Organisation – BSO – has a mobile phone number available for the recipient) with a source identifier on the message 'HSCresult' (to ensure the validity of the message),
  - by email (from the NHS test portal),
  - or by a call (via the PHA manual contact tracing process).

- The contact details are from information volunteered by a person booking a test on the NHS portal, or from existing contact information, held by BSO, volunteered when registering for medical services. No record of the SMS message is retained, once it has been generated and sent. The message of a positive test will contain a random 6 digit alphanumeric 'authorisation code', for input into the app. This code will remain valid for 24 hours.

- For those not able to receive an automated SMS, they will be called directly (routinely via the PHA manual contact tracing process) and as part of the call, will be asked if they are using the app. If so, a SMS can be generated while on the call.

[2] The description of Exposure Notification Services and how it is used in this document is abbreviated and approximate, removing much of the cryptographic underpinnings in an effort to more clearly impart the key matters relating to data protection. For a full explanation of this service please refer to the Google and Apple documentation - https://www.google.com/covid19/exposurenotifications/ | https://www.apple.com/covid19/contacttracing

- When the code is entered into the app, this authorises an upload of their anonymised IDs (or 'identifier beacons') generated by the phone, every 15mn, over the previous 14 days. These IDs are then designated as 'diagnosis keys', and the app user is asked directly via the app to authorise release of the same to the app backend architecture, hosted in a secure environment, in a secure AWS account. On entry to the backend architecture, the IP address is stripped off the 'diagnosis keys' (and not retained anywhere) rendering the 'diagnosis keys' completely anonymised and non-identifiable data).

Figure 2: on positive diagnosis, a person can optionally upload their IDs

- The backend architecture then makes these anonymised 'diagnosis keys' visible to instances of the app on other users phones, covering only the infectious period of 14 days (this is known as 'publication'). This enables other app users who have been in 'high risk' contact with an app user (who has tested positive) to be notified. The app checks newly published 'diagnosis keys' every two hours. If there is a match between stored close contact IDs, ('identifier beacons'), from the previous 14 days, and newly published 'diagnosis keys', an exposure notification is triggered. The notification advises the user to self-isolate for 14days, get a test if they develop symptoms, and provides a link to further information, including a number to call if they have issues relating to the notification. **At no point in the 'exposure notification' process is any identification of app users possible.**

Figure 3: apps download new random 'diagnosis keys' and alerts person if a match is found

- The app has the advantage of notifying 'high risk contacts' who are app users, who may be unknown to the person testing positive. The app improves the possibility of breaking chains of transmission of the viral infection. Notifying unknown 'high risk contacts' in a timely

manner (within a couple of hours of a test result being known). The manual process takes up to 24 hours at present; and in a period of peak demand, this can extend further.

Exposure notifications remain visible on the app for 14 days from the date of last exposure. Users can clear exposure notifications from their app at any time via settings. If a user receives multiple exposure notifications relating to different exposure events, they only receive a new alert if the exposure notification relates to a more recent exposure event.

Any individual in NI can book a test via the national portal. Patients may be advised to get a test via multiple sources: e.g. the 111 helpline, COVID-19 NI smartphone and online app, and normal clinical consultations with a GP, or the GP OOH service. For individuals booking a test via the NHS Portal, they are asked to provide contact details, (phone number or email address) in order to receive a result notification. Results are passed from the National Pathology Exchange (NPEx), to the HSC Test registry hosted and administered by the Business Services Organisation (BSO) who are data processors for this data, on behalf of PHA, the data controller for COVID-19 test data. The portal, and testing data sit outside the app architecture and this processing is covered off under separate Information Governance arrangements, with specific DPIAs and Privacy Notices held by PHA and DHSC. The PHA will also call the person and guide them as per the current contact tracing operations. When someone receives an exposure notification via the app, they are advised to self-isolate and book a test if they become symptomatic. The phone number of the user receiving a notification, or the number of the person testing positive, are not visible via the app, and will not be shared. Furthermore the PHA is not aware of an exposure notification in any way. If a person self-isolating after an 'exposure notification' becomes symptomatic and books a test, should the test be positive, they will be followed up in the manual tracing process. If they are also an app user, and have registered a contact mobile number, they will receive a 6 digit 'authorisation code' for input, independently of the manual contact process.

3.2 Other Functions

Metric Gathering – during the on-boarding process, the app makes the user aware of the collection of metrics, which are only collated at a regional level. This takes place during the on-boarding process, with a clear description of the information recorded. The metrics collected do not reveal a person's identity and are shared on a daily basis with the DoH. The metric data collated is as follows:

- Total number of app downloads / users – data routinely available for any app hosted on an app store – no individual level data is available on this metric.
- Total number of 'authorisation codes' entered, and the total number of exposure notifications delivered – all at a regional level, not individual level. **Collection of this aggregated information is <u>necessary</u> to provide evidence of efficacy for CE accreditation / MHRA regulatory.**

Leave Function – the app provides a leave function that can be used at any time. Selecting this deletes all app data from the phone. The user will be notified that they can also delete ENS data via the phone device settings as the app does not have direct control or access to ENS data. If Leave is selected, non-identifying security token data that is used to associate valid (device integrity checked) apps with the app backend is removed from the app backend. If the app is simply deleted from the phone, it has the same effect as 'Leave', however the security tokens are not removed as the app backend has no way of knowing – they will be deleted after a period of 60 days of not being used.

App Settings – the phone operating system controls Bluetooth and Notifications settings. If these functions are disabled the app alerts the user to this. Enablement of these phone functions enables the following app functions:

- Contact Tracing function is displayed as on or off and the user is directed to the ENS phone settings where it can be turned on or off;
- Exposure notifications can be cleared from the app if relevant;
- A link to 'terms and conditions', and a 'privacy notice'

Share function – the app makes it easy for users to share it with others who may choose to download it also. The success of contact tracing apps relies on widespread adoption by communities who collectively can help protect themselves and others.

3.3 Systems where personal data will be processed

Personal data will be collected, processed and stored in the following locations and IT systems:

1. The app – on users' phones where data is stored and encrypted on the device.
2. The app backend – the backend services are hosted by Amazon Web Services (AWS). The app uploads anonymous IDs (on entry of an 'authorisation code' to affirm a positive test for COVID-19) and the limited metric data to the backend services. The app also downloads IDs for exposure matching from the backend services. All data is encrypted in transit and at rest, and is stored in the AWS London Region.
3. Backend linkage with the RoI backend – to enable interoperability with the ROI, in line with EU recommendations. This is via a 'federated server' hosted on the ROI AWS account in Dublin. See the MOU 'Appendix D'. The 'diagnosis keys' processed by this server are non-identifiable data. The IP address is stripped from the 'diagnosis keys' on entry to the app backend, before the non-identifiable keys are passed on securely to the federated server. The infrastructure us set out in 'Appendix H'

3.4 Technical Data Flows and Architecture

Technical data flows and the technical architecture of the app are set out in 'Appendix H'. A description of separation of support functions, in order to prevent re-identification of data is set out in 'Appendix I'.

4. Scope of Processing

This section of the document describes the data that will be processed, how much data is being collected and used, how often it will be processed, how long it will be retained for, and who the data relates to.

4.1 Data Subjects

The proposed data processing relates to all individuals in the country that choose to download and install the app that have a smartphone capable of meeting the ENS requirements set out previously. The app will be published in the UK and Ireland app stores only, making clear that it is intended for download by individuals residing in Northern Ireland to download and install it. To support contact tracing for app users travelling across the border with the ROI, (it has been estimated that before lockdown, there were 30,000 individuals crossing the border on a daily basis), backend linkage will be enabled (in line with EU recommendations) to deliver interoperability. Cross border interoperability is something that the European Commission and separately Google and Apple are

working on. The DoH is working in cooperation with counterparts in the ROI to deliver interoperability to EU requirements. A MOU has been agreed governing the functioning of the NI / ROI 'federated server' and sharing of anonymised 'diagnosis keys' (see 'Appendix D').

4.2 Data Retention

There are various retention limits on different types of data being processed and these are outlined in tabular form later in this section of the document. An overarching policy of data retention in relation to the app is that no data captured will be processed beyond the period of the pandemic in line with recent European Data Protection Board's guidelines on the introduction of such apps. The terms of reference charge the App Steering Committee to ensure that an orderly wind down of the app and the removal of all data captured is implemented within 90 days of the end of the COVID-19 crisis. The end of the COVID-19 crisis and the wind down of the app will be determined by NI Executive taking advice from the Chief Medical Officer in NI. The wind down will include measures such as of the issuance of clear guidelines for app deletion, removal of the app from app stores, the secure destruction of all captured data and diagnosis keys from backend servers, and the shutting down of all app backend services.

Users of the app have the right to be forgotten. Selecting the Leave function will remove all data held by the app and any security token data on the app backend. The Leave function will also inform the user that ENS is a phone service and will give guidance on how to remove ENS data via the ENS service settings. Deleting the app from your phone will also remove all app data from the phone, and the security token data will be automatically removed 60 days after last use. The removal of all app data and ENS data can be done at any time, and the DoH has no way of knowing who selects Leave or uninstalls the app.

4.3 IP Address

All API calls to the DoH will unavoidably result in app users' IP addresses being present in data communicated between the app and the network servers due to the nature of networking. The DoH will not use IP addresses for identification purposes. As a precaution, IP addresses of users are never transmitted from the networking layer to the backend servers thus minimising the possibility of inadvertently recombining IP address and app generated data. This stripping off of the IP address, on entry to the backend, is a security measure designed to prevent re-identification of data, protecting privacy. The IP addresses which have been removed, are not retained anywhere in the architecture.

Under these circumstances it is reasonable to consider that no personal data is processed by the StopCOVID NI app. Users receive an SMS code to authorise (following a positive test) the upload of random IDs to the registry (anonymous 'diagnosis keys') on the incidence of a positive diagnosis. Users may also be given a code via a phone call or email. Users have the option not to upload these codes. 'Exposure notifications' occur by virtue of the 'publication' of 'diagnosis keys'. Having had the IP address removed in the networking layer, the keys are random identifiers, with no way of connecting them back to source, and as such constitute non-identifiable data. The Gov.UK Notify service, which transmits the SMS message to deliver an 'authorisation code' to authorise release of 'diagnosis keys', is similarly separated from the app backend. As well as designing separation in the backend architecture, consideration has also been given to separation of support arrangements, separate teams managing separate elements to further ensure protection against re-identification of data.

While it is arguable that dynamic IP addresses are not personally identifiable information, however, without prejudice, this DPIA takes a conservative approach and considers IP address as personal data, and thus acts as a personal identifier. As such all app data transferred to and from the DoH

backend servers relating to a person is considered personal data and will be handled as such. This is to ensure compliance with GDPR, and is in line with ICO guidance and more recent rulings.

4.4 Download and Installation

To install the app, a user downloads the app from either the Google or Apple app stores. Each store will keep a record of the user's download of the app using their unique identifier, AppleID or GoogleID, within the store. Apple and Google are Data Controllers in respect of their respective app stores and gather certain statistics about app usage, such as number of downloads and number of deletions. More information is publicly available in regards how data is processed by the app stores.

4.5 Exposure Notification Services

It is worth going into further detail on the workings of the 'exposure notification' service (ENS) at this stage to support the rest of this section. Each phone that has ENS switched on generates a random daily key, which is stored on the phone, and called a 'Temporary Exposure Key' (TEK). These keys are used to further generate random IDs approximately every 15 minutes called 'Rolling Proximity Identifiers' (RPI) (referred to above as 'identifier beacons', or ID 'keys'), which are used to send to other ENS enabled phones when nearby. RPIs are accompanied by Associated Encrypted Metadata data, which includes protocol versioning and Bluetooth transmission power. The TEK keys are uploaded to the DoH on positive diagnosis and are called 'diagnosis keys' at this point. These are publically available, downloaded by all apps, and used to regenerate the RPIs – which are in turn used check for a match, on the phone, in order to generate an exposure notification. RPI and AEM data are processed on phones only; not available directly to contact tracing apps; are stored for 14 days; are not capable of being used to identify a person; and are not considered personal data (the IP address having being deleted at the networking layer as described earlier).

4.6 Personal Data

The following scope for personal data processing has been determined. All data uploaded to the DoH should be considered to have IP addresses removed at the networking layer of the app backend and put beyond use. A rigorous data minimisation approach has been adopted in relation to personal data processing, and only personal data that is necessary for the proper operation of the app will be processed. The following table sets out the personal data that will be processed by the app, along with a description of the data, the type of data, how often the data is processed, who processes it and for how long. A more detailed technical list of all data processed by the app on the phone and on the backend servers will be published online.

Data	Activity	Type	Frequency	Processed By	Retention
'Diagnosis Keys'	On positive diagnosis, an app user is invited by the app to input a randomly generated 6 digit code. For the majority this code is delivered via SMS. A small proportion will be contacted via phone, during manual contact tracing, to be given a code. Only those 'authorisation codes' that are automatically verified in the backend architecture as valid, will be accepted by the app. Gov.UK Notify SMS service is used to deliver the code, using data from the lab 'test registry' (or via call from the contact tracing centre). The user consents to upload their 'diagnosis keys' by typing in a code received by SMS, and selecting the 'yes' option to release them. *The processing of the phone number required to send the SMS is discussed in the next row of this table.*	As this data is only processed when a person is diagnosed positive for COVID-19 it is considered health data. On release from the phone, the data package has an IP address and security tokens attached. This is stripped off and deleted on entry to the network layer, (see below). The resulting 'diagnosis keys' stored in the app registry are truly anonymous.	Once per positive diagnosis of an app user.	The phone generates random IDs privately every day ('identifier beacons'). On positive diagnosis, the app requests permission from the user to access these random IDs from the phone and then shares them with the app backend for publication. All apps download any new IDs from the registry every 2 hours to check on their phone for exposure events. To enable interoperability between NI / ROI app users, a 'federated server' provides secure exchange of 'diagnosis keys' as non-identifiable data, from the app registry of each jurisdiction.	Phones generating random IDs retain the data for 14 days unless the user deletes ENS data via phone settings. The app backend and 'federated server' stores IDs for 14 days. Apps download and process IDs to check for exposure events only for as long as is required to determine if there is a match or not.

SMS Transmission of 'Authorisation Codes'	Based on information submitted by the patient on registering for a test on the NHS portal, or registration data held already in association with registration for health services in NI (enabling the association of test results with existing lab data on electronic patient records): the user will receive an SMS, email or phone call (contact tracer triggering an automated SMS securely) on receipt of a positive diagnosis. If they are an app user, the 'authorisation code' transmitted via SMS can be input on the app UI. The app user will be asked to consent to upload their 'diagnosis keys', inputting an authorisation code into the app UI.	As this data is only processed for a positive case it is considered health data.	Once per positive diagnosis of an app user.	The 'test registry' automatically transmits the mobile phone numbers and date of test (to allow the app user to authenticate the information), via an API, to the SMS server, associating it with an 'authorisation code' from the DoH app backend architecture on AWS. The BSO 'test registry' generates random anonymous 'log IDs' to associate with each instance of SMS generation. Only these anonymous IDs are retained, to allow reconciliation of transmission, assisting in detection of transmission failure.	As soon as the SMS is sent, the phone number and date of test is deleted, and only the anonymous 'log IDs' are preserved. These are deleted following reconciliation that SMS transmission has been successful. Where transmission fails due to an incorrect phone number registered by an individual, there is no technical solution. Safety netting occurs via the manual contact tracing process. The app backend has no way of knowing the phone number of a person that either uploads their keys, or chooses not to upload their keys. The network application, the app backend, the 'test registry' and SMS server are separate applications in the architecture. Re-identification of data is not possible. The log reconciliation, an support function, is merely designed to detect system failures, not errors in mobile numbers provided. All data is deleted as soon as the function it is supporting has been completed. 'Authorisation codes' are valid for 24 hours, and then are deleted in the app backend. SMS messages remain on the user's phone for as long as they wish.

Metrics	Users are made aware during the on-boarding process that metrics data will be collected. They are informed of the type data collected and the purpose – **necessary to gain MHRA regulatory requirement / CE accreditation**. Data metrics collected – total number of users, total number of 'authorisation codes' entered / uploading instances, total number of exposure notifications – all at regional level and not user level.	Some metrics measure counts of exposure notifications or diagnosis key uploads – this data is considered health data, and generated from the app. App store data on total app user downloads is standards as for any app, and is not health data.	In general shared with the DoH daily. This is aggregate data and summary data. None of the data can be linked to an individual.	The DoH processes this data daily and uses it to monitor app effectiveness.	This data is retained by the DOH as anonymous data for statistical and research purposes for a minimum of 7 years and reviewed for further retention at that stage. This aggregate data is retained by the DoH as anonymous data for statistical and research purposes in line with the DoH's retention and disposal policy – Good Management Good Records (GMGR). **The data is necessary to demonstrate effectiveness of the app for MHRA regulatory approval / CE accreditation.**
IP address and app security tokens	User IP address is required for internet traffic and is present at the networking layer of the app backend, but processed no further. Security tokens, which do not reveal identity, but note that the app installed has passed basic and standard phone integrity checks (e.g. a test that the app isn't running on an emulator). This is primarily to stop illegitimate apps being used to attack the app backend APIs.	Considered personal data.	On all app to app backend communication.	The phone and the DoH networking layer in the AWS presence. Not processed in the app backend, to prevent re-identification.	IP address is held in a transient manner on the networking layer for networking and security reasons. It is not persisted, nor logged on the app backend in any other way. The app security tokens are deleted on selection of the Leave function, or the deletion of the app (immediately on the phone, and after 60 days of not being used by the app backend as the backend is not aware of an app being deleted).

5. Context of Processing

This section of the document sets out the relationship the DoH has with data subjects, how much control they have over the data processed, what type of people make up the data subjects. It also sets the context in regards the privacy concerns that people may have with the app. Terms of use and Privacy Notice are available under 'Appendix A'.

5.1 Design Principles

Through how the app is implemented, the app's governance and the supporting communications, we will ensure a set of design principles are adhered to through the design, build and operation of the app. In particular, governance arrangements are in place via an App Steering Committee where the terms of reference charge it to uphold a set of principles. These principles include the following.

- The app is entirely voluntary to use;
- The app is used to augment the existing manual contact tracing process;
- The app is used for the purposes set out in the DPIA, and only in the context of the COVID-19 crisis;
- The app is to be decommissioned once the COVID-19 crisis is over;
- The app processes data as set out in the DPIA and Privacy Notice, the DPIA and Privacy Notice are accessible to the public and kept up to date (see 'Appendix A');
- The app does not use location services to track the location of users or for any other purpose;
- The app does not, and will never, reveal the identity of a person infected with COVID-19;
- The app must be able to function while the screen is locked.

The trust of the public in the proposed processing of data and appropriate privacy measures are of paramount importance to engender adoption of the app. The DoH is committed to transparency in the development and operation of the app and to that end the source code and this DPIA document and related documents will be published to the public online as soon as they are ready. These will be kept up to date to reflect the live operation of the system and the data being processed. Furthermore, robust processes will be put in place to perform security testing and respond to security issues during the development and the operation of the app.

5.2 Privacy Model

As mentioned previously, the Contact Tracing function uses a new Android and iPhone service called 'Exposure Notification Service's (ENS). Only nationally recognised health authorities will be able to produce an app that is authorised to use ENS. Apps that do use ENS have limited levels of access to ENS data. Examples of this includes – apps are not allowed direct access to the random IDs being exchanged with nearby phones (RPIs) (referred to in this document as 'identifier beacons' and ID 'keys'); they are restricted in checking for exposure matches a maximum of 15 times per day; and they cannot get access to diagnosis keys without the user's explicit permission. In general apps are restricted in how they can use ENS in order to preserve the privacy design of the service. ENS follows what is informally called a 'decentralised' model for mobile app contact tracing, which allows people to get exposure notifications without sharing personal data with a health authority or anyone else. The DoH is committed to this design principle. The DoH will independently test the robustness and security of the ENS service. The Expert Advisory Group (see 'Appendix A' will help provide an oversight function: source code data has been made available to the ICO for scrutiny as part of the process of transparency).

5.3 Children

In line with UK legislation, safeguarding protections would be necessary for individuals under the age of 18 years using the app, necessitating parental consent. This would be problematic as there is no definitive age for children's consent within the UK; and due to anonymity built in to the app (by design to be GDPR compliant), gaining parental consent would not be possible. Due to the need for anonymity there won't be any facility for direct contact with users, or a mechanism to monitor this. The DoH would have no way of checking a child's capacity to consent. For that reason, prospective app users will be asked to confirm that they are 18 years or older at the time of downloading the app. Enforcing this is also problematic. App store controls will be put in place to restrict availability of the app to the extent that is possible. Google play store can restrict downloads from aged 17 and above; the Apple app store can restrict from aged 18 and above – these settings will be applied. Due to the overriding nature of the need to deliver a proximity app solution that meets ICO guidance for anonymity, there is no identified mechanism for further age verification possible. It is seen as a significant challenge to reliably seek parental consent to support younger users of the app at this stage. It is not clear at this time how this can be achieved in a practical way that can scale. Furthermore, it is not clear the appropriateness of alerting young people with exposure notifications as they may not be in the presence of a guardian at the time. As it is in the public interest to have a first release of the app available to the public in NI as soon as possible, (supporting contact tracing measures to reduce COVID-19 transmission as 'lockdown restrictions' are released) the app will be released with an age challenge included, asking the user to affirm that they are 18 years of age, or older. It is not perceived that any harm will result for individuals younger than 18 years of age using the app, due to the protections built in to protect privacy. Consultation will be undertaken with the Northern Ireland Commissioner for Children and Young People to explore options for inclusion of individuals younger than 18 years of age, while meeting the complex competing requirements of inclusion, safeguarding and anonymity. Having taken advice, the DoH will commit to implementing any agreed modifications in subsequent releases of the app, post launch. Inclusion of individuals under the age of 18, at the earliest possible juncture, is a priority for the DoH.

5.4 Novelty and Robustness

The DoH is heavily engaged with other countries who are introducing similar apps to help stop the spread of the virus. As this use of phones is new, this type of engagement is important, and the project team will continue to engage, contribute and learn from others in the field. Furthermore, the team are in regular contact with Google and Apple, working with these companies to shape the design and functioning of ENS to maximise the value to society and people's health, while protecting the rights to privacy. The use of ENS is considered the best route to a robust working version of the Contact Tracing function. ENS is to provide the ability for apps that implement contact tracing to be functional on both Android and iPhone devices, with the app running in both in the background and foreground; a significant challenge to date. Furthermore, it is expected from discussions with Apple and Google that ENS will be heavily optimised and tested for efficient battery use and will not interfere with other Bluetooth peripherals – also a significant challenge to date for current contact tracing apps.

The DoH has engaged in its own testing (directing services from independent private sector companies, Expleo and IT Guarded, offering expertise in assurance process and security penetration testing) of the app to ensure the product is robust, reliable, and privacy preserving, including testing in a Northern Irish specific context. Following launch of the app, the DoH will engage with colleagues in the ROI to provide testing for QA purposes, to ensure functioning interoperability and optimal deployment. Prior to launch, interoperability has been tested, and proven to work. The post-launch

work will aim to ensure optimisation. The scientific community continues to play an important role in the Northern Irish response to Covid-19. The University of Ulster and Queen's University Belfast are both represented on the App Steering Committee, providing expert advice and oversight (see 'Appendix A').

5.5 Accessibility

The app has been carefully designed to be clear and transparent in how it works, to ensure consent, where sought, can be freely given, to make it possible for people to opt in (and out) of the functions provided, and to update their data at any time.

User Experience of the app has been tested within behavioural studies informing the app flow and content. There is little interaction required for setting up the Contact Tracing function, no identifiable user data input is required, and it can run in the background without user interaction – thus reducing to as much as is possible any barriers to entry. Accessibility testing has been included in the QA assessment of the 'User Interface' (UI) prior to the initial app release, and will be for subsequent releases (updates). In future, development of Irish language version, and support of other commonly used languages within the country will also be considered.

6. Stakeholder Engagement

A series of public and stakeholder consultation meetings were undertaken, to help inform the development and subsequent deployment of the app. The purpose of these consultations was to gather views, perspectives, and experiences from experts, and members of the public, on a range of interrelated issues. From a development perspective, the following issues were explored: privacy, appropriate use of data, cybersecurity, data accuracy, and accessibility. From a societal perspective, the following issues were assessed: social inequalities, ethical implications, engagement with health services, and user expectations, needs and engagement. As part of the engagement, a second cycle of meetings was arranged, to demonstrate to stakeholders that their concerns had been listened to and addressed. Feedback on this process has been positive.

6.1 Public advocacy representatives

DoH has been engaging with:

ICO	Social Change Initiative
Privacy Advisory Committee	Women's resource and development association
Human Rights Commissioner NI	Older People's Commissioner
Amnesty	Committee for the Administration of Justice
Human Rights Consortium	NBI Human Right Commission
Equality Coalition	Children's Law Centre
NICVA	Children's Commissioner

6.2 Consultation with the ICO in NI

The 'StopCOVID NI' has been developed in line with the ICO published recommendations "COVID-19 Contact tracing: data protection ICO on app development".

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/covid-19-contact-tracing-data-protection-expectations-on-app-development/

The ICO regulates and enforces the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA). The ICO is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations and taking appropriate action where the law is broken.

The DoH has been actively engaging with the ICO to ensure that the StopCOVID NI app has been developed in line with the GDPR and the DPA 2018, so that individuals can be assured that their personal data is protected. The ICO has been given access to the app source code for purposes of verification. The DPIA and correspondence with the ICO will be published, in order to support launch of the app, promoting trust and confidence on the part of the public; and hopefully ensuring widespread download and adoption of the app.

6.3 Engaging the scientific community

An 'Expert Advisory Group' has been constituted, and meeting formally on a weekly basis, commencing 3rd July 2020. The group comprises academic representatives, with expertise in technology, and cybersecurity, from both universities in NI, QUB and UU (along with DoH representation). Members have been kindly donating their time, in order to support the DoH in this endeavour. They have played an important role, providing independent oversight and assurance, on behalf of the NI population, assisting the DoH to develop and deliver a digital proximity smartphone app, as part of the response to COVID-19. They will also be key stakeholders in design and delivery of a research programme post-launch, to evidence the efficacy of the app. The 'terms of reference' for this group are appended ('Appendix A').

7. Compliance with data protection law and other regulatory guidance

This section considers compliance with GDPR, the Data Protection Act 2018, other related legal obligations and data protection guidelines.

7.1 Legislative Framework

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 together form a framework for regulating the processing of personal data in the UK from 25th May 2018.

In relation to 'Metrics' and 'IP address and app security tokens' the '**processing is necessary for the performance of a task carried out in the public interest**' as per GDPR Article 6(1)(e). The legal basis for the data processing is The Health and Social Care (Reform) Act (Northern Ireland) 2009,

- Section 2(1) the duty to promote in Northern Ireland an integrated system of health care designed to secure improvement in the physical and mental health of people in Northern Ireland and in the prevention, diagnosis and treatment of illness, and
- Section 2(3)(g) the duty to secure the commissioning and development of programmes and initiatives conducive to the improvement of the health and social well-being of people in Northern Ireland, and
- Section 3(1)(b) the power to provide, or secure provision of, such health and social care as it considers appropriate for the purpose of discharging its duty under section 2; and

do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of that duty.

In relation to Special Category data, Article 9(2)(i) applies to the processing, **'processing is necessary for reasons of public interest in the area of public health'**. Under DPA 2018, Schedule 1, Part 1 condition 3 is met in relation to Article 9 as follows:

Public health

3 .This condition is met if the processing—

(a)is necessary for reasons of public interest in the area of public health, and

(b)is carried out—

(i)by or under the responsibility of a health professional, or

(ii)by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

The app cannot function beyond the initial 6 month MHRA Exemption from device regulation during COVID-19 without attaining CE accreditation. The metrics data, collected at a regional level, are essential in demonstrating efficacy (which will be essential for attaining accreditation). The app cannot be used beyond the 6 month exemption without accreditation. A mobile smartphone **cannot** link via a network to transfer data without use of an IP address and app security tokens. This information is deleted at the earliest opportunity and not stored anywhere in the infrastructure.

'Diagnosis Keys' are released from the phone by the permission of the data subject. They are essential for letting others know that they are at risk of having been infected via the 'exposure notification' process. A person using the app may receive 'exposure notifications' by using the app, utilising the published 'diagnosis keys' of others. They may however decline to enter and 'authorisation code' on receipt of a positive test result, or may decline to release their 'diagnosis keys' for publication. While it is not anticipated that anyone would wish to use the app in such a manner, it is technically the position that release of 'diagnosis keys' is not essential for an app user to consent to this publication process, in order for them to benefit from notification by others. Technically it is arguable that at the point where 'diagnosis keys' exit a user's phone, they are associated with an IP address and app security tokens, and as such are personally identifiable. Though IP addresses vary, and are not static, some more recent rulings have deemed them 'personally identifiable'. Once the IP address and app security tokens have been deleted on entry to the networking layer, the 'diagnosis keys' are non-identifiable. Once stored in the app registry, the 'diagnosis keys' are clearly non-identifiable, and can be published without risk of re-identification. The app is voluntary to use and the legal basis for the processing of the 'diagnosis keys' is 'consent', namely GDPR 6(1) (a), and GDPR 9(2) (a), 'explicit consent', in relation to the processing of special category data. Consent is sought for release of the 'diagnosis keys' on the app at the point of release.

The following sets out the legal bases for the processing of personal data identified in Section 4 of this document. The processing activity is included in brief for convenience.

Data	Activity	Legal Basis
Diagnosis Keys	On positive diagnosis, the user can give their permission to share their diagnosis keys with the DoH for publication, and access by other app users. These are potentially identifiable until the IP address and app security tokens are deleted (see below)	These keys indicate the health status of the person. Permission is sought before processing. The sharing of the 'diagnosis keys is a key component of the 'exposure notification' process and is essential in delivering the public health function of reducing spread of infection by asymptomatic individuals: essential in the public health role of pandemic response. The app is voluntary to use and the legal basis for the processing of the data is 'consent', namely GDPR 6.1.a, GDPR 9.2.a.
	The published diagnosis keys are downloaded by all apps to check for a match (indicating a 'high risk' contact likely to result in infection)	On upload to the app backend, the IP address is deleted, and the resulting non-identifiable keys are distributed to apps via a registry. The data is considered anonymous at this stage. As such processing falls outside of scope of GDPR.
IP address and app security tokens	The data is part of the normal secure transfer of data and network connectivity and network traffic.	The identifiable data is stripped off in the networking layer of the architecture, at the point of entry, and is never passed to the app backend. It is not stored anywhere. It is not possible for any app to operate with connectivity and avoid transmission of such data. The legal basis for the processing of the data is 'processing is necessary for the performance of a task carried out in the public interest' and 'for public interest in the area of public health' – namely GDPR 6.1.e, GDPR 9.2.i.
Metrics See 'Page 10' for full breakdown.	This data is collected by the DoH at a regional level and is non-identifiable.	High level aggregated regional data is collected to demonstrate the efficacy of the app. This is vital to prove clinical effectiveness in post-deployment regulatory approval. The legal basis for the processing of the data is 'processing is necessary for the performance of a task carried out in the public interest' and 'for public interest in the area of public health' – namely GDPR 6.1.e, GDPR 9.2.i.
	This data will be shared by DoH with the HSCB, and used for reporting oversight to the NI Assembly Health Committee.	The data that is shared with the HSCB does not include the user's IP address and is considered anonymous. As such processing falls outside of scope of GDPR.

7.2 Privacy and Electronic Communications Regulations 2003 (as amended) ('PECR')

The app involves gaining access to data already stored on the phone (e.g. app metrics, keys upload, authorisation code upload) and storing data on the phone (i.e. random ID exchanges) using a webservice and an electronic communications network, and as such PECR 2003 applies. All data that falls under this in regards the app is deemed strictly necessary in order to provide a service explicitly requested by a user, and as such the exemption set out in regulation 6 of PECR 2003 applies. This

includes is metric data, essential for continued viability of the app beyond the 6 month MHRA 'Exemption from device regulation during COVID-19', when CE accreditation will be required to be in place. The metrics collected in the app, previously listed, are essential to evidence effectiveness in terms of its primary function; and will be essential for attaining CE accreditation. App users are explicitly informed of the scope of the metrics collected, and the purpose of collecting that data, during the on-boarding process.

The MHRA guidance on medical devices states:

- "The software must meet all of the general essential requirements and the relevant design and construction essential requirements contained in annex I of the directive. This guidance lists those essential requirements that are likely to apply to software and apps."

General Requirement 3 within Annex I of the Medical Devices Directive states:

- "The devices must achieve the performances intended by the manufacturer and be designed, manufactured and packaged in such a way that they are suitable for one or more of the functions referred to in Article 1(2)(a), as specified by the manufacturer."

7.3 Role of the HSCB

Anonymous aggregated data (regional level and not individual or specific) as outlined previously (above) in this document will be shared with the HSCB for the purposes of statistical reporting and analysis. The DoH will work with the HSCB in the creation of statistical reports to inform the CMO, DoH and various public health teams on COVID-19 response policy making and measurement. The Committee for Health, NI Assembly, has specifically requested regular reports on the performance of the App.

7.4 Necessity and Proportionality Assessment

Necessity of processing requires that the proposed measures to be introduced will be effective for the objective pursued and whether it is less intrusive compared to other options for achieving the same goal. Proportionality of processing requires that the advantages of the processing proposed are not outweighed by the disadvantages the measures may cause to a person's rights, and as such, a balance must be struck between the means used and the intended aim.

Necessity and Contact Tracing – the need to operate a form of contact tracing during the COVID-19 pandemic is beyond doubt. The basic operating principle is that on diagnosing a person with the disease, the close contacts of that person are identified, generally through interviews, and appropriate measures are taken in respect of those persons so identified to control the spread of the disease. This is an effective intervention in the fight against COVID-19 and has been deployed worldwide. However, there are inherent challenges to manual contact tracing.

In a review of international literature it was found that manual forms of contact tracing are overly reliant on recall (Leong et al., 2009) and it is argued that, for a highly infectious disease with a long incubation period, capacity to recall decreases and the likelihood of the disease being spread beyond known and usual contacts increases (Hart et al., April 2020). Furthermore, manual contact tracing also requires substantial human resources in the form of contact tracers (Hart et al., April 2020). Emerging literature suggests that manual contact tracing procedures is too slow, lacks efficiency, and occurs at too small a scale to contain Covid-19 (Ferretti et al., March 2020, Hinch et al., April 2020). Additional measures have been introduced in Northern Ireland, and other countries, to aid in the

control of the virus, such as severely restricting persons' movements, working habits and general day to day activities.

Key indicators of effective contact tracing are completeness of close contact identification and speed of close contact identification and subsequent follow-up, with a view to quickly and significantly reduce the viral transmission potential. The objective of using a mobile app based contact tracing solution as a supplement to the existing manual contact tracing is to increase the completeness of close contacts identified, and increase the speed in which those close contacts are identified and given the appropriate guidance.

Recently published data from the ONS survey has demonstrated that up to 79% of those who have a positive test result, have no symptoms on the day of testing, and no idea that they are infected. This means that the majority of people who have COVID-19 have no idea that they have it. To stop the infection spreading it is essential that those who do have symptoms get a test, and that if they test positive, we can identify people they have been in close contact with (<2m distance and >15min duration) so that they can be notified to self-isolate and avoid spreading the virus. This should take place as early as possible because most of those who are infected won't know it, and are likely spreading infection unknowingly. Identifying close contacts and advising them to self-isolate as early as possible is an effective approach to infection control.

Independent SAGE has advised that to be effective in slowing the spread of COVID-19, contact tracing should aim to identify 80% of close contacts. Manual contact tracing has been demonstrated to help reduce spread if infection, but relies on people knowing those that they have been in close contact with, in order for them to be contacted. As we come out of lockdown, the number of people we are in close contact with will increase substantially, as will the proportion of people we are in contact with who are unknown to us. Manual contact tracing cannot possibly reach people unknown to us, so manual contact tracing cannot possibly deliver 80% achievement. Deployment of the 'StopCOVID NI' smartphone app, helping to notify people who we may have been in close contact with, (but don't know), should we become infected, can provide a significant intervention in breaking chains of infection, in parallel to the manual contact process. The automated process of notification can significantly speed up the process of notification, compared to manual processes.

It is significant to note that the DoH is intending to introduce an app based on the Apple and Google's ENS service. Apps introduced in other countries to date have not been so based (as ENS hasn't been available), and have had significant functional difficulties, namely not functioning, or severely hampered functioning, on iPhones, issues with battery life, and interference problems with Bluetooth peripherals. Furthermore, these apps have generally been based on a 'centralised' approach, where the public health authority require access to significant amount of contact tracing data of positive and close contacts, for which there have been privacy concerns raised. Concerns over these factors may have hampered adoption. The app recently deployed in the ROI was based on a 'decentralised' model. The level of uptake has been significant and rapid, with approximately 30% of the population downloading and installing the app within two weeks of launch (indicating significant levels of public confidence).

The use of ENS is intended to solve the referenced issues regarding the basic core functionality proposition of proximity detection. Furthermore it is based on the decentralised model, removing the need to share contact traces with a central authority. It is also expected that as more and more countries adopt the ENS service, which there is considerable momentum towards across the EU, a consolidation of improvements in product robustness and interoperability across borders will emerge. Alternative approaches to meeting the objectives stated above included the use of a

centralised model and GPS/location tracking, and while certain benefits prevail over the proposed approach for NI (namely assistance in cluster identification), significant privacy concerns exist with these approaches and they are not being pursued. The StopCOVID NI app will be launched with interoperability between it and the ROI app. This is a significant development, supporting cross-border travel, and helping reduce chains of transmission traversing the border. The MOU governing this arrangement is appended ('Appendix D').

Governance safeguards to limit the scope and extent of interference with data protection and privacy rights are in place through the terms of reference of the Expert Advisory Group (see 'Appendix A'), ensuring data is processed in line with its purpose and principles, including the full wind-down of data processing when the COVID-19 crisis is over, and the ongoing monitoring of the effectiveness of the app and appropriate wind-down if it is not. Through the design and implementation of the Contact Tracing function these rights are further protected by ensuring it is, and continues to be, entirely voluntary in nature; and that users are asked for their clear and explicit consent if they wish to turn on ENS, and upload their diagnosis keys.

Location services are never used to track the location of users, where instead Bluetooth is used to detect proximity without any location data, meeting its purpose in a data minimised way. Consent can be withdrawn at any time for the processing of all Contact Tracing data and can be deleted under the control of the data subject, independently and without the knowledge of the DoH. There is no consequence to not using the app as the DoH cannot tell who has and who hasn't installed the app. Having taken into account the necessity set out above and the limited interference with data subject rights, the processing proposed under the Contact Tracing function of the app is seen as necessary and proportionate.

Necessity and proportionality of App metrics – the processing of app metric data is a supporting form of processing for the performance of the above functions and to monitor their effectiveness. It is also intended to give the public health teams insights into the functioning of the app, such as the number of exposure notifications per day, for use in health policy formulation and measurement. It does not collect, nor share personally identifiable information. Users receive information in relation to the collection of the data during the 'on-boarding' process, and can decide to remove the app from their pone at any time. It is considered to have little interference with individuals' rights, and is seen as necessary and proportionate. The data collected is essential in proving efficacy, essential for regulatory approval and the continued availability of the app.

7.5 Technical and Organisational Measures

Technical and organisational measures will be put in place prior to the launch of the app to ensure the information processed in relation to the COVID Proximity app is carried out only as detailed in this DPIA and ultimately only for the purposes intended. The DOH is designing, developing and putting in place the required organisational measures to ensure the privacy preserving approach to the app and the protection of the fundamental rights of individuals to privacy and data protection are established and maintained.

The organisational security measures implemented include the following.

- The DoH has engaged a specialist information security advisory at an early stage in the design, development, testing and operational planning of the app. The company providing this service is a National Cyber Security Centre (NCSC) approved service provider. Support has been provided directly by the NCSC, in oversight of penetration testing process, and advising on likely threats and mitigations.

- An appropriate separation of roles will be employed, for example developers will manage the app supporting backend architecture, and the BSOs team will manage the central 'test registry' and provide support for the Goc.UK Notify SMS text service. This avoids potential re-identification of data.
- The app will be independently tested from an information security perspective. This will include the app on the phone and the app backend services. An independent company has been engaged to provide assurance testing.
- All access to the app backend databases on AWS will be logged and the audit trails of this activity will be preserved. Audit logs of access are captured and will be reviewed for compliance by BSO IT Security, on behalf of the DoH.

The app backend uses Amazon Web Services (AWS) London Region (via a Health & Social Care Board NI account) and the highly available services that it provides, and in so doing, the DoH has ensured an appropriate level of availability of the backend infrastructure to support the potential high level of take-up of the app. All services will be configured with appropriate availability groups in the London region data centre from AWS, and ensure the data resides only in Northern Ireland administered presence on the AWS facility. The use of AWS ensures that the solution can scale up and down in an elastic fashion to deal with demand.

Technical privacy and security measures are implemented via encryption at a number of levels and include the following.

- Data in the app - all data that is gathered and stored on the phone will be encrypted. On both the iOS and Android devices, the encrypted data will only be accessible once the app is launched, and then only by the app itself. The encryption does not rely on the device level encryption that may or may not be enabled on the device itself. All ENS data – Diagnosis Keys, Rolling Proximity Identifiers, and Associated Encrypted Metadata – are stored encrypted by the phone's Exposure Notification Services.
- Data in transit – the data being transferred from the app to the app backend is encrypted using TLS v1.2 in transit. Minimum TLS and cipher requirements are defined to prevent weak ciphers being used and leaving to potential for a "man in the middle" attack. The app will implement certificate pinning to ensure that the only site it will negotiate a TLS session with is the COVID Proximity App backend in AWS and not any other TLS enabled service. This also ensures that only COVID Proximity Apps will be able to negotiate a session with the AWS backend and limit any potential attack surface and removes the potential for attackers to flood the app backend with fraudulent symptom data.
- Data in the app backend – once the data has been received by the networking and routing layer of the app backend and processed; it will then be transferred to a database where it will be stored in an encrypted format. This database is not accessible from the Internet and is only accessible on a private network connection in AWS, from application servers in London. Identifiable information such as IP addresses are stripped from the data at point of entry to the networking and routing layer. The identifiable information is not retained. Non-identifiable data is passed to the app database.

A number of security hardening measures are in place to protect against malicious actors, these include the following.

- The DoH has engaged a Penetration Test and Application Security team to analyse the app code prior to release and ensure the technical security measures have been implemented correctly.
- This team will also perform Penetration Testing and Application Security Testing on the AWS

API gateway (this is the service that the app communicates with in the app backend).

- Web Application Firewall is implemented to provide an application layer assessment of API traffic to remove potential threats prior to the data being processed by the API gateway.
- Continuous Vulnerability Assessment will be engaged for the API gateway and AWS services for as long as the service remains active.
- The team will be analysing the Bluetooth communications for Exposure Notification Services to ensure the integrity of the user device is maintained. The design of the app and contact tracing ensures that there is no requirement to "pair" the device from a Bluetooth perspective.

The app backend processes data in a secure manner, ensuring that inappropriate access is restricted at all times. The following sections speak to the various data sent by the app to the app backend.

Diagnosis Keys – a request for Diagnosis Keys is triggered by the manual contact tracing operations based on a positive test result as part of COVID-19 core clinical pathway. The lab test centre in BSO will securely send the phone number from positive tests only to the app backend SMS solution. The SMS solution will request a 6 digit alphanumeric code for input from the app backend. The SMS service (a backend application hosted on the AWS account) will send an SMS message with the code to the phone. The app backend retains the code and this is stored for verification, in app backend, along with the date. The phone number, and SMS, is removed from the SMS solution at this stage. The code and date is retained for a maximum of 24 hours.

The app user receives an authorisation code (following a positive test result), entering it in app UI and consents to upload diagnosis keys. The app then calls an app backend API using an HTTPS POST with the Diagnosis Keys and the code. The app backend ensures a code match, and uses the date information to store the appropriate Diagnosis Keys in the Diagnosis Key Registry. The code and date information is deleted from the app backend at this stage. A Web Application Firewall is used to monitor across all API services in particular the diagnosis key upload API for malicious activity.

App indicators and metrics – this data once received by the app backend is transmitted securely to the DoH. The app backend will expose a secure REST API, to allow the metrics data to be accessed, on a daily basis. The data is encrypted with the CSO Public Key. The data is retained by DoH for 24 hours from the day of receipt in case in order to facilitate the transfer of the data to the HSCB. The data can be accessed by DoH / HSCB operations staff in appropriate roles. These roles are authorised by the DoH CDIO. Audit logs of access are captured and reviewed for compliance by BSO IT Security.

IP address and security tokens – as mentioned previously and noting here for completeness, IP addresses are processed in the app backend at the networking layer and no further for the purposes of networking and network security only. The IP address is not logged on any service by the app backend. Also, as mentioned, security tokens are created to protect the app backend from malicious actors. The first connection of an app to the app backend contains security measures such as ensuring the device is valid and not an emulator or a bot. This establishes the means of validating subsequent traffic from the app over its lifetime.

7.6 Exercise of Data Subject Rights

Users have rights under GDPR when their personal data are processed by data controllers. The following considerations should be noted. IP addresses are not retained on the app backend, but for transient network routing and network security purposes. Diagnosis keys are not capable of being associated with a person as they are non-identifying by design.

Right to information – a Data Protection Privacy Notice (Notice) is provided via the app itself on those pages which request information and also in the app Settings. The Privacy Notice will also be published on the DoH website. The Notice contains information as prescribed under Article 13 and 14 of the GDPR.

Right to rectification – since no personal data is collected or retained by DoH, it would not be possible for DoH to comply with a request for rectification.

Right of access – since no personal data is collected or retained by DoH, it would not be possible for DoH to comply with a request for access.

Right to erasure – the user can select the Leave function, delete the app at any time, and delete ENS data via device settings – erasing all data processed on the phone. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for erasure.

Right to restriction – the user can revoke their ENS permission, revoke their exposure notification permission and decide not to upload keys. Ultimately the user can decide to Leave and/or delete the App from their device. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for restriction.

Right to portability – it is not possible for users to port their keys, for example, from one device to another device as the user does not have access to such keys on their device (save to delete them) and as regards those uploaded to the DoH, the DoH cannot identify which keys belong to which user. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for portability.

Right to object – the user can use the Leave function to delete the information from the app; the user can delete the app from their device and the user can delete ENS data via device settings.

Right not to be subject to solely automated decision-making including profiling – if the ENS detects a match between a Rolling Proximity Identifier on the App and a Diagnosis Key downloaded from DoH Diagnosis Key Registry, a decision is made that a close contact has taken place. This decision is based solely on the automated processing of identifiers and keys and does significantly affect users. However, this processing is based on the explicit informed consent of the user, during the on-boarding process. The automated decision-making is an essential feature of the proximity app solution provided, and is core to nits function in delivering the public health objective of infection control. If App users wish to speak to someone in relation to an 'Exposure Notification' that they have received via the App, they can call '0300 200 7896' and select the option to speak to someone about the notification at the following times: Monday-Friday (excluding bank holidays) between the hours of 830am – 530 pm. Someone will answer the call and explain the 'Exposure Notification'. They will have no way of knowing with whom, where or when the 'high risk' contact took place, but they will try to explain the process to App users and its purpose. **App users can express their point of view and contest the decision.** These steps should enable the App user to make an informed decision as to whether to self-isolate to prevent spreading the infection to others. Ultimately if they are still not satisfied or need clinical advice they will be advised to seek clinical assessment by their GP or GP OOH (See 'Appendix C').

7.7 International Transfers

There will be no international transfers of data. The AWS account is hosted in London region. The BSO servers infrastructure is hosted in Belfast. The backend integration with the ROI to support interoperability is hosted within the EU and is GDPR compliant. It appears likely that Germany will

host a federated server for Europe to support European interoperability. Once this becomes available, the backend infrastructure on AWS will be linked to this server to support pan European interoperability.

7.8 Appointment of Data Processors

All of the data processors are appointed under Data Processors Agreements in compliance with Article 28 of the GDPR.

8. Identify and Assess Risks

Appendix E sets out the risks that have been identified for the project and the levels for those risks *if not mitigated*. Overall risk score for each risk identified is calculated as the product of the risk likelihood score and the risk impact score (i.e. likelihood score X impact score). The following sets out the metrics used in documenting the risk assessment.

Likelihood	Score
Highly Unlikely	1
Unlikely	2
Possible	3
Likely	4
Highly Likely	5

Impact	Score
Negligible	1
Minor	2
Moderate	3
Major	4
Critical	5

Overall	Score
Low	1-7
Medium	8-14
High	15-25

9. Identify Measures to Reduce Risks

An evaluation of the identified risks in the previous section has been carried out and a series of measures have been detailed that seek to mitigate those risks to an acceptable level. The table in Appendix F sets out these mitigation measures and an assessment of the risk impact due to their introduction. The table also sets out if these mitigation measures have been approved.

Appendix A - COVID Proximity App Steering Committee - Terms of Reference

Northern Ireland 'StopCOVID NI'

Expert Advisory Group

Terms of reference

09/07/2020

Purpose

To provide independent oversight and assurance, on behalf of the NI population, assisting the DoH to develop and deliver a digital proximity smartphone app, as part of the response to COVID-19.

Scope

Under the 'Test Trace and Protect' (TTP) project, the DoH has undertaken (in partnership with a number of private sector companies) to design, develop and deliver a smartphone proximity app, providing a digital means of augmenting the manual contact tracing process. TTP is aimed at breaking chains of transmission of COVID-19 in NI, by identifying 'high risk' contacts of individuals who have tested positive for COVID-19, encouraging them to self-isolate to avoid passing on infection to others.

The 'StopCOVID NI' app being developed by the DoH, utilises the Google-Apple API, utilising a decentralised architecture in line with ICO recommendations for GDPR compliance. Private companies have been engaged to provide assurance testing, including a NCSC approved provider of security penetration testing of the app, and backend architecture. These companies will hold primary responsibility in assuring the security and functioning of the app, and associated supporting architecture. Due to the sensitivity of this project, the potential for reputational harm, and the potential for any failure to undermine public trust in the DoH, (in relation to managing the COVID-19 response,) it was considered prudent to have an additional level of independent assurance.

Version 3.0 Final 09/07/2020

This expert advisory group has been convened to meet the following objectives:

- Review the assurance testing process, advising the DoH on issues identified and appropriate mitigations
- Provide analysis of the solution design, advising the DoH on fitness for purpose and compliance with GDPR requirements
- Provide analysis of the programming code used, advising the DoH on fitness for purpose and compliance with GDPR requirements
- Provide further analysis and advice in relation to any future updates of the app, advising the DoH on continuing fitness for purpose and GDPR compliance
- On the occasion of the COVID-19 pandemic being declared officially ended, provide independent oversight and assurance that the project has been decommissioned, with appropriate deletion of any remaining data (in line with GDPR / ICO requirements)

Membership

- Dan West CDIO
- David Wilson QUB
- Edward O'Neill, Product Manager
- James McLaughlin UU
- Máire O'Neill QUB
- William Burns UU

Meetings

Meetings will be held weekly by video, initially, until the app is launched. Dates and times tbc

Further meetings will be agreed as necessary, following launch of the app.

Secretariat

Action points will be recorded at each meeting.

Appendix B – Data Processors and Sub-Processors

Data Processors and Sub-Processors

The following provides a list of data processors and sub-processors involved in the delivery of the app. All data processors and sub-processor arrangements are managed via GDPR compliant agreements and contracts.

Amazon Web Services (AWS) processes the information uploaded from devices. AWS process the data as a sub processor contracted by the Health and Social Care Board (HSCB), which are a data processor on behalf of the Department**.**

Health and Social Care Board (HSCB) owns the AWS account which hosts the app. HSCB act as a data processor on behalf of DoH.in providing this service and the services provided by NearForm, BSO and Gov.UK Notify (see below).They are also responsible for managing the contracts with these providers.

NearForm were chosen to develop the App and are regarded as a sub-processor contracted by the HSCB, on behalf of DoH as. They will also provide support on an ongoing basis to the app supporting architecture, for the duration of its operation, as part of their contract.

Business Services Organisation statutory organisation providing services as a data processor for HSCB and PHA. They host the test registry for lab results, and provide backup support to the SMS function, through arrangements with the HSCB.

Gov.UK Notify provide the SMS text messaging service used to distribute 'authorisation codes' to those testing positive for COVID-19. They are a sub-processor contracted by HSCB (to provide this service.

Kainos have developed the IT platform (utilising Microsoft Dynamics) used to support the manual contact tracing process (for the Public Health Agency NI) [covered by a separate DPIA]. Via this platform, professional staff in the PHA conducting manual contact tracing will have the ability to trigger a SMS text message, to be sent to those who test positive for COVID-19, who are using the app, but have been unable to enter an 'authorisation code' for whatever reason. PHA are the data controller for this information, under existing contact tracing arrangements and Kainos is a data processor on behalf of PHA.

DoH Ireland

Host the 'federated server' and are a data controller in their own right. There is a MoU to govern the sharing of anonymised diagnosis keys to the federated server, between DoH NI and DoH IRL, (see Appendix D).

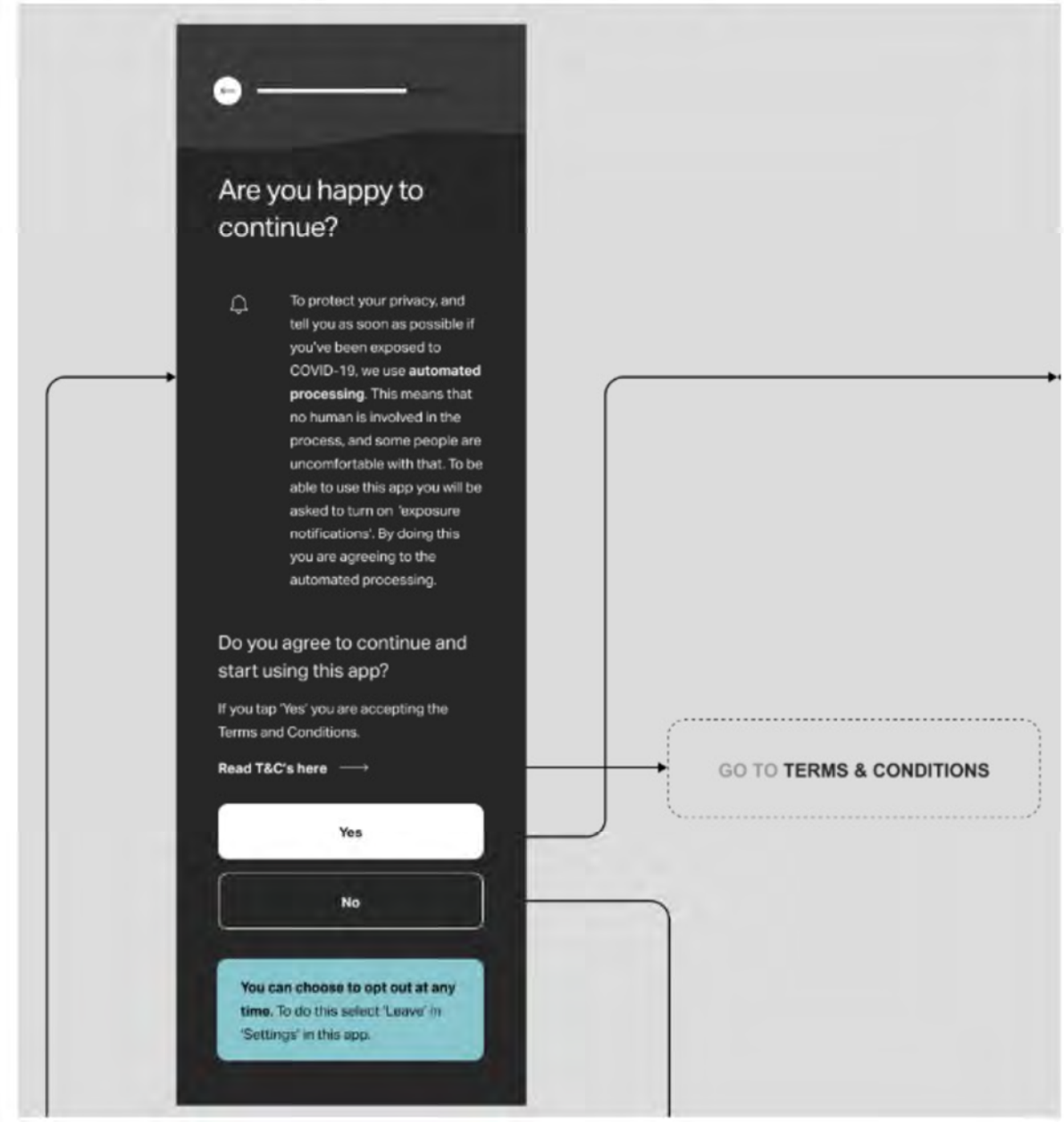
Apple and Google

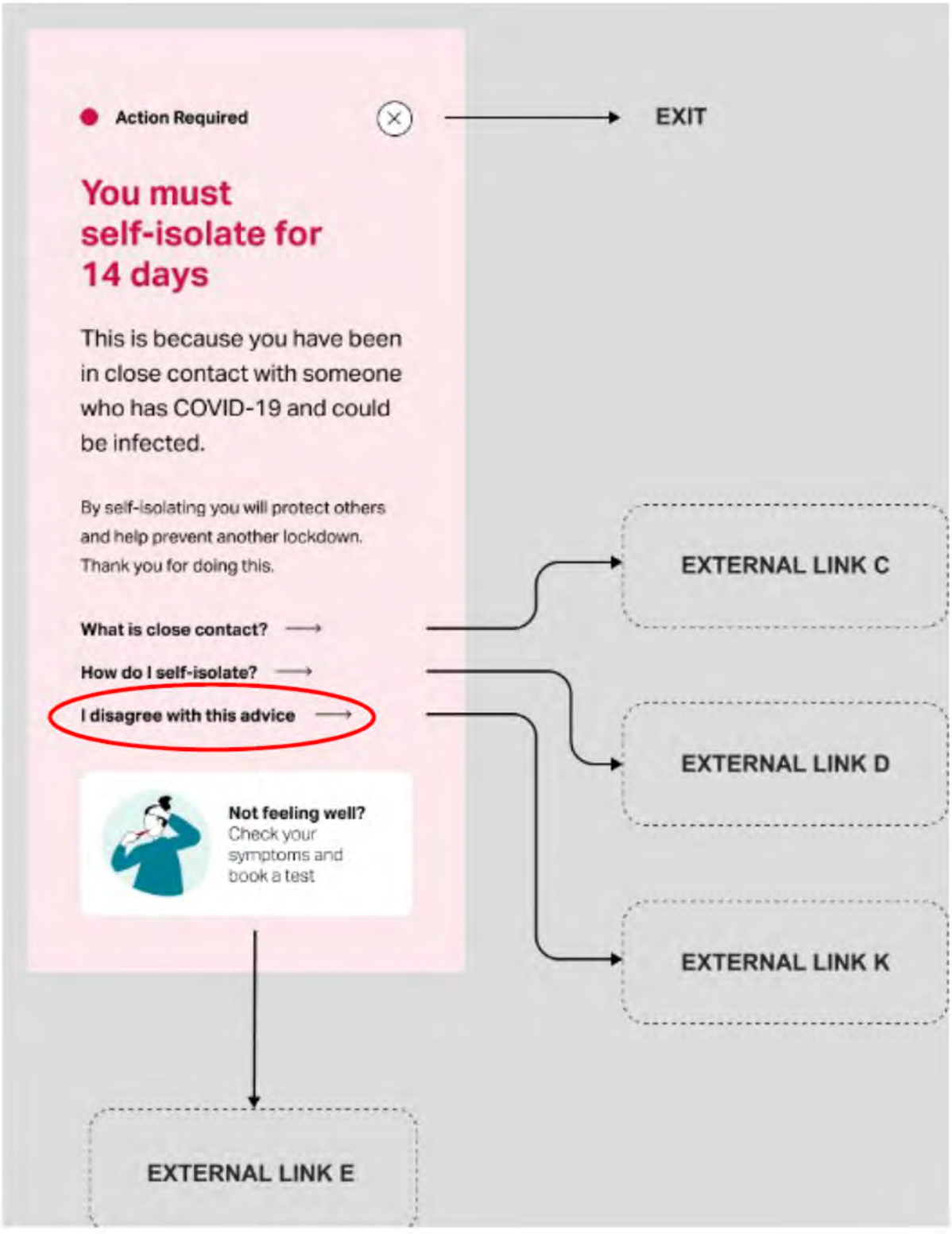
The following is a note on Apple and Google's role.

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. This processing activity is separate to the processing of personal data on the app. Furthermore, although Apple and Google have developed a COVID-19 Exposure Notification Services service, which is used in the app, neither company obtain any information from the app or the Exposure Notification Services service itself.

Appendix C – Automated Decision-Making

Within the App, the following screens refer to 'automated processing'.





External Link K will link to the Following text.

Automated Individual Decision-Making

Under the provisions of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, (for regulating the processing of personal data in the UK from 25 May 2018, replacing the former Data Protection Act 1998); Article 22 affords the following protection:

"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

This may not apply if you have given explicit consent and if there is access to a human to speak to in order to express your point of view and to contest the decision.

In accordance with this, we have put the following measures in place, to ensure that your rights are not infringed. During the on-boarding process, in activating the App, we asked you to consent to the automated processing of your information that would be involved in you receiving an 'Exposure Notification' and being advised to self-isolate. The processes involved in detecting significant contact episodes between App users, and using these to determine risk of infection should one or other test positive for COVID-19, are clearly explained in the 'Terms & Conditions' and 'Privacy Notice' The DoH's prime concern in designing how the StopCOVID NI App operates was to preserve anonymity, and ensure that 'Exposure Notifications' could be facilitated, without the collection or transmission of any personally identifiable data. Automated decision-making within the App is essential, in order to avoid needing to share your identity, or the identity of other App users.

The App 'Exposure Notification' process mirrors the manual contact tracing process, in terms of estimating the risk of transmission of COVID-19 as being related to a 'high risk' contact; within 2 metres in terms of distance, and for 15 minutes, or longer, in terms of duration. If you receive an 'Exposure Notification', it means that at some time in the previous 14 days, you had a 'high risk' contact with someone who has now tested positive for COVID-19. That means you are at high risk of having been infected with COVID-19 and there is a high risk of you passing the infection to others (**even if you have no symptoms**). Recent information published by the Office for National Statistics indicates that 79% of those who test positive for COVID-19 have no symptoms at the time of testing. In order to slow the spread of the virus, we need to use the manual contact tracing process and the App (working in parallel) to let those who have had 'high risk' contact, with someone who has tested positive, know that they are at risk of having been infected, and should self-isolate to avoid passing it on to others.

The App achieves this in an anonymised manner to protect your identity, and the identity of other App users. If you receive an 'Exposure Notification' via the App, we will have no way of knowing with whom, where or when the 'high risk' contact took place. If you wish to speak to someone in relation to an 'Exposure Notification' that you have received via the App, you can do this by calling '**0300 200 7896**' and selecting the option to speak to someone about the notification at the following times: Monday-Friday (excluding bank holidays) between the hours of 8:30am – 5:30 pm. Someone will answer your call and explain the 'Exposure Notification'. They will have no way of knowing with whom, where or when the 'high risk' contact took place, but they will try to explain the process to you and its purpose, to allow you to understand it, and make an informed decision as to whether to self-isolate to prevent you from spreading the infection to others. **App users can express their point of view and contest the decision.** If you have a clinical concern, you should contact a clinical professional for advice.

Appendix D – MOU for the 'Federated Server' DRAFT

Memorandum of Understanding between the Department of Health Ireland and the Department of Health Northern Ireland for the sharing of anonymous 'diagnosis keys' generated by each jurisdiction's COVID-19 Proximity Apps

Version Number	Date	Prepared by	Classification
1.0	22.07.20	Dr EGJ O'Neill	Draft
1.1	23.07.20	Dr EGJ O'Neill Charlene McQuillan	Draft
2.0	23.07.20	Peter Lennon Owen Harrison Niall Sinnott	Draft
3.0	24.07.20	Peter Lennon Charlene McQuillan	Draft
3.1	25.07.20	Nicola McAlister	Draft
4.0	25.07.20	Dr EGJ O'Neill	Draft
4.1	27.07.20	Niall Sinnott	Draft
4.2	29.07.20	Niall Sinnott	Final

Final 25/07/2020 v4.0

Department of Health
An Roinn Sláinte
Männystrie O Poustie
www.health-ni.gov.uk

1.0 Background and Context

1.1 The Departments of Health, Northern Ireland (NI) and Ireland (IRL), each have a statutory responsibility for the health and wellbeing of the populations they serve. There is also existing and long-established cooperation on the island of Ireland between the Departments and the health services as well as strong cooperation between the respective offices of the Chief Medical Officers in both jurisdictions.

1.2 That cooperation is at the centre of the ***Memorandum of Understanding -COVID-19 Response: Public Health Cooperation on an All-Ireland Basis -between the Department of Health, Ireland (and its Agencies) and the Department of Health, Northern Ireland (and its Agencies)*** (April 2020). That Memorandum formally recorded the mutual willingness of the parties to promote cooperation and collaboration in response to the COVID-19 pandemic and explicitly acknowledged the compelling case for strong cooperation in public health measures (including information-sharing) and, where appropriate, a common approach by the parties to action in both jurisdictions.

1.3 Accordingly, this present ***Memorandum of Understanding for the sharing of anonymous 'diagnosis keys' generated by each jurisdiction's COVID-19 Proximity Apps*** is directly derived from the commitments in that April 2020 Memorandum. On that basis, the matters to which this Memorandum relates are, therefore, an action within the power of the respective Ministers for Health. In preparing the Memorandum careful consideration was given to whether additional authority was required for the sharing of any information.

1.4 The Departments of Health IRL, and NI, in jointly preparing this Memorandum are acting to give effect to the respective decisions of the Irish Government and NI Executive, in relation to each jurisdiction's Covid-19 Contact Tracing App / Proximity App, which have mandated the delivery of interoperability on an all-island basis.

1.5 In accordance with the above, and to ensure that the sharing of the anonymous 'diagnosis keys' (generated by each jurisdiction's proximity app, developed as part of the COVID-19 Contact Tracing Programmes in Northern Ireland and Ireland,) is managed within an agreed and transparent protocol, this Memorandum sets out the specific reciprocal arrangements for such sharing.

1.6 The purpose is to support interoperability between the NI and IRL apps, allowing users from each jurisdiction to use their app in support of travel across the border, in either direction. Facilitation of this operational feature will allow the apps of both jurisdictions to support digital measures (to provide 'exposure notifications' to those who have been in close contact with someone who has tested positive for COVID-19) aimed at breaking cross-border chains of transmission. Prior to 'lockdown' measures, there were an estimated 30,000 persons travelling across the border daily. Developing effective measures to limit the potential for cross-border spread of infection is very much in the interest of citizens of both jurisdictions. As 'lockdown' restrictions ease, increased cross-border travel is inevitable. If measures to reduce the transmission of COVID-19 are to be effective, epidemiological solutions, which span both jurisdictions, are essential.

1.7 From the outset, it was established that a core requirement in the development of the Contact Tracing Apps in each jurisdiction was that participation must be voluntary and consent based both in terms of downloading the app and in relation to the processing of any personal data associated with the app. That emphasis is reflected in the respective Data Protection Impact Assessments undertaken and in the related app Privacy Notices.

1.8 Accordingly, it was considered essential that there should be a full examination and consideration of whether the proposed sharing arrangement set out in this Memorandum would involve the transfer of personal data within the meaning of Article 4 of the General Data Protection Regulation 2016. The outcome of that process is that anonymised information rather than personal data will be shared. The rationale for that conclusion is found in the details provided in the paragraphs below (detailing the type of data being shared). Further, and in keeping with the transparency that has underpinned the development of the app in both jurisdictions, the respective DPIAs and Privacy Notices will be amended so all individuals downloading or using the apps will be fully informed in relation to any decisions they make notwithstanding that personal data is not involved.

2.0 Data being shared

2.1 The phones of those who are using the apps emit anonymised coded 'keys', 'Identifier Beacons', which change every 15 minutes. These 'keys' are stored on the user's phone for 14 days before being discarded. When close to each other, app users' phones exchange these anonymous 'keys', and if they are in close proximity with another user for a significant period of time, both will store the anonymous 'key' of the other phone for 14 days.

2.2 'Authorisation Codes' are anonymous random six digit /alphanumeric codes generated to verify that a positive test has been received by the app user, allowing 'exposure notifications' to be sent via the app, when the user enters a valid 'authorisation code.' On entering the code, the user is asked to release keys that can be used to generate the anonymous keys their phone has transmitted over the previous 14 days: these keys are then known as 'diagnosis keys'. These are then released to a secure registry supporting users of the apps to be shared with other app users.

2.3 'Diagnosis keys' are anonymised identifiers uploaded on entry of an 'authorisation code'. For the NI App, these keys are stored in a secure registry, maintained in a Health & Social Care Board secure cloud services account (on behalf of the DoH NI) on Amazon Web Services (AWS) (based in London). A similar process is followed in relation to the IRL app, where the IRL registry, is hosted on the AWS presence based in Dublin. Every app user's phone regularly checks for 'diagnosis keys' from their respective registry and where these generate a match of a significant contact episode's anonymous 'key' stored on their phone over the previous 14 days, an 'exposure notification' is enabled. The notification is generated on the user's phone, not in the secure registries.

2.4 Where 'Exposure Notification' is mentioned, this refers to an anonymous notification received, via the app, that you have been in contact with an unnamed individual who has tested positive for COVID-19, and that contact was recent enough, and for sufficient time, at a close enough distance to mean that you may have been infected.

2.5 To allow digital proximity app solutions to work in support of cross-border travel requires the sharing of 'diagnosis keys' cross-border, in a shared (federated) server. This will allow sharing with app users, from either jurisdiction, enabling an 'exposure notification' to be triggered, irrespective of which app is being used, when app users have been in close proximity (2m or less) for sufficient duration (15mins or more).

2.6 The 'diagnosis keys' are released on an informed basis by app users. They are stripped of IP information on entry to the AWS backend supporting the apps in both NI and the IRL. IP addresses are not stored or logged. As such these anonymous 'keys' are non-identifiable, and re-identification is not possible. Users' apps, in this arrangement, will be able to process 'diagnosis keys' from both jurisdictions, against 'keys' exchanged in line with each jurisdiction's close contact policy, irrespective of which app is being used. Processing is locked down and not visible to app users. They have no visibility of 'identifier beacons' nor diagnosis keys on their phone. The processes are automated within the app, and not visible

to the app user. The exchange of 'diagnosis keys' will take place on a 'federated' server, in a separate fargate cluster, hosted on the Dublin AWS presence. As such it is secure and separate from either app backend.

2.7 'Diagnosis keys' published on the federated server will be automatically deleted after 14 days.

3.0 Purpose

3.1 By virtue of the provisions of the 2005 International Health Regulations (IHR), national health protection bodies are obliged to work with colleagues in other member states. The Health Protection teams in Northern Ireland and Ireland work collaboratively in adherence to current practice, responding to the COVID-19 pandemic, supporting a manual contact tracing process that involves cross-border cooperation.

3.2 This Memorandum aims to support a similar agreement in respect of the exchange of anonymous 'diagnosis keys', supporting interoperability of the apps developed by the DoH NI and DoH IRL.

4.0 Aim

4.1 The aim is to have an agreement in place to ensure contact tracing apps can work on an all island basis by sharing anonymised information pursuant to the health and wellbeing of citizens in NI and IRL, supporting interoperability of digital proximity app solutions and assisting in infection control measures in response to the COVID-19 pandemic. This document commits both parties to ensuring delivery of that function, protecting the citizens of each jurisdiction and ensuring that no identifiable information is shared as part of this agreed process.

5.0 Key actions and communications

5.1-

a. Both parties will ensure appropriate completion of a DPIA in order that there is open and transparent declaration of intent. They will also undertake consultation with the Data Protection Commission and Information Commissioner, as appropriate, in each respective jurisdiction, to ensure data protection compliance.

b. Both parties will ensure that app users are appropriately informed in making their decisions to facilitate the data exchange.

c. Both parties will ensure that the data shared is anonymised prior to exchange, and as such the data cannot be used in isolation or in combination with any other data at any stage thereafter to identify a person by either party or any third party.

d. Both parties will ensure that the data shared, namely the 'diagnosis keys', relate only to persons that have been diagnosed positive for COVID-19 by the respective public health authorities.

6.0 Duration of the agreement

6.1 This agreement will remain in place for the duration of the COVID-19 pandemic. The 'federated' server will then be decommissioned. Periodic review will be undertaken on a six monthly basis, the first review being on 17th January 2021, or in the context of significant material alteration to policy for management of the COVID-19 pandemic response, in either jurisdiction.

7.0 EU Exit

7.1 Both parties will continue to share the data specified in the Memorandum for the purpose of protecting their respective populations from COVID-19 in the event of the UK exiting the EU without an agreement, as set out in the [AGREEMENT on the withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (2019/C 384 I/01)].

8.0 NON-BINDING

This Memorandum represents the common understanding of the parties to the matters referred to herein. It is not intended to create legally binding rights or obligations on any party. Further, it does not constitute an international agreement and does not create rights and obligations governed by international law.

Note: This MOU is a live document and is subject to review by the parties

Signed by

For Ireland

Final 25/07/2020 v4.0

Dr Ronan Glynn
Acting Chief Medical Officer
On behalf of the Minister for Health

Date: 30/07/20

For Northern Ireland

Dr Michael McBride
Chief Medical Officer
On behalf of the Minister for Health

Date: 30/07/20

Final 25/07/2020 v4.0

Appendix E – App Metrics

Data	Activity	Type	Frequency	Processed By	Retention
'Diagnosis Keys'	On positive diagnosis, an app user is invited by the app to input a randomly generated 6 digit code. For the majority this code is delivered via SMS. A small proportion will be contacted via phone, during manual contact tracing, to be given a code. Only those 'authorisation codes' that are automatically verified in the backend architecture as valid, will be accepted by the app. Gov.UK Notify SMS service is used to deliver the code, using data from the lab 'test registry' (or via call from the contact tracing centre). The user consents to upload their 'diagnosis keys' by typing in a code received by SMS, and expressing explicit consent on-screen. *The processing of the phone number required to send the SMS is discussed in the next row of this table.*	As this data is only processed when a person is diagnosed positive for COVID-19 it is considered health data.	Once per positive diagnosis of an app user.	The phone generates random IDs privately every day ('identifier beacons'). On positive diagnosis, the app requests permission from the user to access these random IDs from the phone and then shares them with the app backend for publication. All apps download any new IDs from the registry every 2 hours to check on their phone for exposure events. To enable interoperability between NI / ROI app users, a 'federated server' provides secure exchange of 'diagnosis keys' as non-identifiable data.	Phones generating random IDs retain the data for 14 days unless the user deletes ENS data via phone settings. The app backend and 'federated server' stores IDs for 14 days. Apps download and process IDs to check for exposure events only for as long as is required to determine if there is a match or not.

SMS Transmission of 'Authorisation Codes'	Based on information submitted by the patient on registering for a test on the NHS portal, or registration data held already in association with registration for health services in NI (enabling the association of test results with existing lab data on electronic patient records): the user will receive an SMS, email or phone call (contact tracer triggering an automated SMS securely) on receipt of a positive diagnosis. If they are an app user, the 'authorisation code' transmitted via SMS can be input on the app UI. The app user will be asked to consent to upload their 'diagnosis keys', inputting an authorisation code into the app UI.	As this data is only processed for a positive case it is considered health data.	Once per positive diagnosis of an app user.	The 'test registry' automatically transmits the mobile phone numbers and date of test (to allow the app user to authenticate the information), via an API, to the SMS server, associating it with an 'authorisation code' from the DoH app backend architecture on AWS. The BSO 'test registry' generates random anonymous 'log IDs' to associate with each instance of SMS generation. Only these anonymous IDs are retained, to allow reconciliation of transmission, assisting in detection of transmission failure.	As soon as the SMS is sent, the phone number and date of test is deleted, and only the anonymous 'log IDs' are preserved. These are deleted following reconciliation that SMS transmission has been successful. Where transmission fails due to an incorrect phone number registered by an individual, there is no technical solution. Safety netting occurs via the manual contact tracing process. The app backend has no way of knowing the phone number of a person that either uploads their keys, or chooses not to upload their keys. The network application, the app backend, the 'test registry' and SMS server are separate applications in the architecture. Re-identification of data is not possible. The log reconciliation, an support function, is merely designed to detect system failures, not errors in mobile numbers provided. All data is deleted as soon as the function it is supporting has been completed. 'Authorisation codes' are valid for 24 hours, and then are deleted in the app backend. SMS messages remain on the user's phone for as long as they wish.

Metrics	Users are made aware during the on-boarding process of the data collected and the purpose – to assess effectiveness in support of MHRA regulatory requirement / CE accreditation. Data metrics collected – total number of users, total number of 'authorisation codes' entered / uploading instances, total number of exposure notifications – all at regional level and not user level.	Some metrics measure counts of exposure notifications or diagnosis key uploads – this data is considered health data. App store data on total app user downloads is standards as for any app, and is not health data.	In general shared with the DoH daily. This is aggregate data and summary data. None of the data can be accessed linked to an individual.	The DoH processes this data daily and uses it to monitor app effectiveness.	This data is retained by the DOH as anonymous data for statistical and research purposes for a minimum of 7 years and reviewed for further retention at that stage. This aggregate data is retained by the DoH as anonymous data for statistical and research purposes in line with the DoH's retention and disposal policy – Good Management Good Records (GMGR).
IP address and app security tokens	User IP address is required for internet traffic and is present at the networking layer of the app backend, but processed no further. Security tokens, which do not reveal identity, but note that the app installed has passed basic and standard phone integrity checks (e.g. a test that the app isn't running on an emulator). This is primarily to stop illegitimate apps being used to attack the app backend APIs.	Considered personal data.	On all app to app backend communication.	The phone and the DoH networking layer in the AWS presence. Not processed in the app backend, to prevent re-identification.	IP address is held in a transient manner on the networking layer for networking and security reasons. It is not persisted, nor logged on the app backend in any other way. The app security tokens are deleted on selection of the Leave function, or the deletion of the app (immediately on the phone, and after 60 days of not being used by the app backend as the backend is not aware of an app being deleted).

Appendix F – Identified Risks

The following sets out the *unmitigated* risks that have been identified for the project.

No.	Risk	Likelihood	Impact	Likelihood Score	Impact Score	Overall Risk
1	The app is a COVID-19 pandemic response app. The purpose of the app is to support and augment the DoH's COVID-19 pandemic response efforts through the use of a mobile app. There is a risk that the scope of the purpose will increase to include, for example use by other public bodies, or for enforcement purposes	If the app is successful there is a high risk that other uses will be seen as attractive to introduce. Also, uses may include informal use in the private sector for purposes the app is not intended for	Any increase in app purposes has the potential to impact all users of the app, and to potentially undermine public confidence in the app	4	5	20
2	Data may be collected about children in the app. How will the app determine the age of the user and how will child consent be collected brings additional risks	If unmitigated it is certain that children, under the digital age of consent, will attempt to use the app	Data would be processed potentially on the basis of consent without it being validly collected; unsupervised reception of an exposure notification may not be understood or may cause disproportionate alarm without a guardian present to assist	5	4	20

3	Risk that suitable ways of withdrawing consent are not built into the app in particular as consent is used as a legal basis for data processing	It is very likely that data subjects will seek to withdraw consent and if not provided for explicitly and carefully via mitigation there is a high likelihood of manifestation of risk	Data subjects have a right to withdraw consent at any time. Inability to exercise this right in an easy and cost-free manner would be a serious breach of data subjects' rights.	5	4	20
4	There is a risk of pollution of diagnosis keys due to bad actors	It is somewhat likely that someone will try to inject bad data into the diagnosis key registry	This would compromise the system and at scale would undermine it resulting in many false exposure notifications and high impact on users	4	5	20
5	Users losing control of their mobile device allowing people to see personal, and sensitive personal data.	Highly likely that this will happen to a small number of people.	If this occurs, users may have their test result, or an exposure notification warning accessed by third parties, known or unknown to them, and suffer distress.	4	4	16

6	A pandemic response app may not give sufficient benefits to support the case for the proposed large scale data processing	The introduction of a novel approach to contact tracing using technology in a novel manner give rise to a significant risk.	The potential for mass processing of data by the DoH could have a significant impact on the rights of data subjects	4	4	16
7	Sufficient people must use the App in order for it to make an effective contribution to contact tracing. Consideration must be given to what part of the population cannot use the App, e.g. people with no or outdated device, children etc. The risk is that data is collected about a proportion of the population but does not bring the expected benefits.	There is evidence from other countries that take-up of the App has been slower than they expected	If limited number of people use the app then it calls into question whether the data processing in the App is necessary.	4	4	16

8	Risk that the Bluetooth proximity and power measurements record that a close contact occurred however a false positive was recorded e.g. reading was made through wall/glass and the person was not a genuine close contact	While Bluetooth is the more accurate solution compared to other solutions available, it is not absolute	People would be designated as being in close contact with a person infected with COVID-19 and asked to follow public health guidelines, including quarantine	4	4	16
9	Risk that the Bluetooth proximity and power measurements do not record that a close contact occurred and no contact is recorded when a positive contact actually did occur (a false negative).	While Bluetooth is the more accurate solution compared to other solutions available, it is not absolute	People who have been in close contact are not identified and asked to self-isolate potentially spreading the virus	4	4	16
10	Risk of insecure methods of data transfer are used that allow access to user's symptoms, or any other data transferred to the DoH (if it could be identified as coming from their specific phone).	Likely that attempts will be made to intercept transfers	Special category data from proximity app needs to be transferred securely.	4	4	16

11	Effectiveness in border areas where people live and work either side of borders could undermine effectiveness and thus justification of data processing proposed	The likelihood of this risk occurring is high for a number of people	The impact on effectiveness of app for those that live for example in Ireland and work in Northern Ireland, and vice versa in regards the Contact Tracing function would be significant. Similarly for those on holidays or indeed also working or visiting other countries regularly, or visitors from other countries to Ireland would be significantly impacted	4	4	16
12	Risk that bundling of related features in the pandemic response app infringes on the data protection principle of data minimisation	Without careful consideration and design the likelihood of this occurring is high as the app	The impact would be a potential infringement for all users that would wish to not participate in all functions provided by the app	4	4	16
13	The use of analytic data gathered from the device for the purposes of how the users interact with the app, daily use, app abandonment, contacts, exposure events, etc., is not anonymous and unexpected to the users. Risk to users that data is not anonymous.	Unmitigated, there are possibilities to intentionally and/or unintentionally use metric data from the device for purposes other than the stated intent	If metric data is inappropriately processed, it could have a significant impact on data subject rights and also greatly undermine users confidence in the app	3	5	15

14	Users are not given sufficient information about how the app works, what data will be collected and for what purpose in a comprehensive way	The requirement to have excellent communications about the app is understood	If the transparency information is not provided in a comprehensive way then this will impact the number of people who will use the app and as consent is used as a legal basis can lead to it not being given without being fully informed	3	5	15
15	Risk that Contact Tracing can be used to identify and track people's location and for profiling purposes, rather than tracking the virus	Uploaded contact traces or data in relation to contact occurrences may be difficult to protect against re-identification and tracking	If conducted then there would be a major risk to the data subjects and their right to privacy	3	5	15
16	As the app knows when a person is uploading their diagnosis keys, risk the app can be used to display the COVID-19 status of a person and be used outside of its purpose	If any COVID-19 status is visible in the app, it is possible it will be used	A third party could attempt to make decisions about the data subject based on their COVID-19 status as recorded in the app.	3	5	15
17	The use of the app may continue indefinitely or longer than justified by the defined purposes	If unmitigated, the app could continue to operate on people's phone unless a positive intervention is put in place	Swapping of random IDs could continue and statistical data continue to be gathered without a supporting purpose. Exposure notifications wouldn't occur assuming manual contact tracing operations cease.	3	4	12

18	IP address is present in all data transfers from the app to the app backend	Apps are often designed to capture information from the mobile device such as the device IP address	The capture of IP address and other identifiers from the device permit the data subject to be identified	3	4	12
19	The risk that SMS code provider can identify that particular person with particular notifications and then infer the COVID-19 positive status of the device owner	The App will send and receive one time codes so this risk is likely to occur. There is a need for an Authorisation token to prevent spamming of the API. The use of push notifications via SMS is the optimum method of doing this.	There would major impact for users if they could be tracked.	4	3	12
20	Technical issues with the app that would reduce function or interfere in a negative way in the working of the other phone's function, thus reducing user engagement, lessening the app's effectiveness, and weakening the case for data being processed.	App could have potential issues around a. Technical – users blame the App for loss of battery life or other similar issues b. Usage – the operation of the App is hindered by the interface with the mobile device operating system	Technical issues with the App reduce user engagement and lessen its effectiveness in providing contact trace data.	4	3	12
21	Role of Apple and Google may process data in a non-privacy enhancing way in the future, or in a way that is not desirable in respect of the rights of data subjects, that is unexpected	Exposure Notification Services from the start has been designed to protect privacy in a data minimised way, in line with the EDPB guidelines from the start of their endeavour	If Apple or Google started to gather and use contacts data for their own purposes form within the Exposure Notification Service this could impact on individuals' data protection rights.	2	5	10
22	Integrity of data is compromised. The diagnosis keys, or mobile number uploaded to BSO servers is erroneous or corrupted, meaning it is unusable or unreliable.	Unlikely to happen if standard development practices are followed	If this happened on a large scale contact tracing efforts could be negatively impacted and users might lose confidence in the app.	2	5	10

23	Users may decide to turn off the Bluetooth service on their phones for battery life or other reasons.	Users have the ability to turn on or off various services on their phones and are somewhat likely to do so.	Turning off Bluetooth would disable the Contact Tracing function	3	3	9
24	Continually downloading Diagnosis Keys may consume a user's network data allowance.	Some users may still be on Internet packages that have a low monthly data limit.	This could incur additional costs for the user.	3	3	9
25	Users can't exercise their data protection rights or don't know where to go to exercise them.	The requirement to be able to allow users to exercise their rights is well known and reasonably unlikely.	Failure to provide for users rights would have a major impact on users and affect the number of people who will use the app	2	4	8
26	Failure to separate the backend architecture and support staffing could compromise anonymity allowing 're-identification' of data	Without specific measures in place to address this, the potential is significant	Significant loss of public trust in the event of a data breach, people removing the app from their phone	4	5	20
27	SMS messaging failure could be missed by the system, meaning that app users don't have a code to put into the app when they test positive	Without mitigation the potential of the app to prevent spread of COVID-19 could be undermined	App fails to alert close contacts leading to increased COVID-19 spread and reputational damage to the app, impacting use adversely	4	4	20

Appendix G – Mitigated Risks

The following table sets out the risks identified for the projects, measures to mitigate these risks and whether those measures have been approved.

No.	Risk	Measures to Mitigate Risk	Likelihood with measures in place	Impact with measures in place	Residual Risk	Measures approved	Remaining risk to data subjects
1	The app is a COVID-19 pandemic response app. The purpose of the app is to support and augment the DOH's COVID-19 pandemic response efforts through the use of a mobile app. There is a risk that the scope of the purpose will increase to include, for example use by other public bodies, or for enforcement purposes, or for other purposes not in line with the original purpose	- Implement clear and transparent communication including DPIA and source code publication - Terms of reference of the App Governance Committee to include the purposes and to charge the Committee with ensuring data is processed in line with those purposes and any changes are carefully assessed, are lawful, are lawfully introduced, and reflected in the DPIA - Ongoing assessment of the app, the data it processes and in particular an ongoing assessment for changes from an ethical, data and privacy perspective - Ensure app is entirely voluntary to use - Monitor continuously for misuse that violates the app's voluntary nature with a view to legislating if required to protect this design principle - Charge Governance Committee with wind down once the COVID-19 crisis is over	2	1	2	Yes	Little risk remaining to data subjects if all measures are implemented as all changes require to respect legislation, and informal (outside of public bodies) use will be protected if misuse is detected
2	Data may be collected about children in the app. How will the app determine the age of the user and how will child consent be collected brings additional risks	- The app will check that age is 18 years or older at the start of the on-boarding journey after installing the app. - The integration with the app stores will prevent the use of the app by children under the age of 18 on the Google Play Store; and under the age of 17 on the Apple App Store - Communication to ensure parents understand the age intention of the app	3	2	6	Yes	Scope of children at risk is significantly reduced with the introduction of mitigants, though not entirely. To be kept under close reviewed during rollout of the app. We will engage with the NI commissioner to review this decision.

3	Risk that suitable ways of withdrawing consent are not built into the app in particular as consent is used as a legal basis for data processing	- App to provide full transparency and information as part of the on-boarding process, highlighting the option to leave and withdraw consent - Use the Leave option on the app - this will delete any personal data held on the mobile phone, and any data that can be linked to their phone on the app backend (i.e. security tokens) - Delete the app from their mobile phone at any time - will leave security tokens for 60 days until removed from lack of use	1	1	1	Yes	Introduction of mitigants through careful design ensures that it is clear for users how to withdraw consent at any time to their data being processed
4	There is a risk of pollution of diagnosis keys due to bad actors	- Put in place an appropriate DoH authorisation step so that only those authorised as having tested positive for the virus can upload their keys - Ensure network and WAF security measures are put in place to block attacks of scale - Ensure device integrity checks are first performed by the app during the on boarding, and to ensure for all traffic to the app backend is protected via this means	1	1	1	Yes	After mitigation it is unlikely to occur
5	Users losing control of their mobile device allowing people to see personal, and sensitive personal data.	- Ensure app can run in the background and when locked (current apps on iPhone require running unlocked at significant risk). - The communications plan for the app will remind people that they should take suitable precautions to protect their mobile device. - The minimising of information captured and used by the app reduces the risk	3	2	6	Yes	This risk remains as the symptom data is in the App and even with a clear communication plan other people will have access to user's mobile phones.

6	A pandemic response app may not give sufficient benefits to support the case for the proposed large scale data processing	- Carry out of an analysis of benefits to support the introduction of an app is to be carried out and inform launch decision. - Use decentralised model to reduce data processed directly by DoH - Use new Apple/Google ENS to significantly increase likelihood of product robustness. - Continued engagement with scientific and other groups to carry out research to continuously assess benefits and effectiveness. - Inclusion in TORs for App Governance Committee to monitor effectiveness and benefits and to wind-down processing if appropriate. - Implementation of a robust testing ahead of launch to the public - Engage intensively with other countries to align and to increase awareness and understanding of approaches used - Ensure app is entirely voluntary	2	1	2	Yes	The analysis and testing ahead of launch along with appropriate ongoing governance to measure effectiveness with appropriate sunset significantly reduces the likelihood and impact of this risk.
7	Sufficient people must use the App in order for it to make an effective contribution to contact tracing. Consideration must be given to what part of the population cannot use the App, e.g. people with no or outdated device, children etc. The risk is that data is collected about a proportion of the population but does not bring the expected benefits.	- Terms of Governance Committee to ensure Committee continuously monitor and assess for impact and effectiveness including adoption and to wind down of app if considered ineffective - Use Apple/Google Exposure Notification Services to remove technical problems that are significantly undermining bespoke Bluetooth implementations of the Contact Tracing function - The app is to be used to augment the processing of the existing manual contact tracing process to ensure that all people are included in a form of contact tracing, where app assists in this process - Ensure effective communications strategy to maximise potential for adoption - Stakeholder engagement to gauge public appetite and perception to app to confirm potential	2	1	2	Yes	Combination of measures once implemented will increase confidence and function of the product, assess appetite potential ahead of launch, and put ongoing measures to assess and review.

8	Risk that the Bluetooth proximity and power measurements record that a close contact occurred however a false positive was recorded e.g. reading was made through wall/glass and the person was not a genuine close contact	- Engage in comprehensive testing with the app and in an Irish environment - Use ENS to benefit from extensive capability of Google and Apple to do extensive testing - Create a well-designed communication plan to ensure those that may be susceptible to causing false positives understand what they can do (e.g. Bus or taxi driver to turn off Contact Tracing while working) - Introduce anonymous metrics to gauge the rate of app based close contacts numbers to app based diagnosed positives to monitor for over reporting of close contacts	2	3	6	Yes	There is still a risk that people would be designated a close contact in limited cases where they should not have been
9	Risk that the Bluetooth proximity and power measurements do not record that a close contact occurred and no contact is recorded when a positive contact actually did occur (a false negative).	- Ensure app is used to augment the existing contact tracing operation - Engage in comprehensive testing with the app and in an Irish environment - Use ENS to benefit from extensive capability of Google and Apple to do extensive testing - Create a well-designed communication plan to ensure those that may be susceptible to causing false positives understand what they can do (e.g. Bus or taxi driver to turn off Contact Tracing while working) - Introduce anonymous metrics to gauge the rate of app based close contacts numbers to app based diagnosed positives to monitor for under reporting of close contacts	2	3	6	Yes	Implementation of mitigation measures will greatly reduce the likelihood and impact, in particular ensuring that the app compliments and does not replace manual contact tracing
10	Risk of insecure methods of data transfer are used that allow access to any data transferred to the DoH (if it could be identified as coming from their specific phone).	- Ensure data is encrypted on the mobile device, in transit over the network, and at the DoH app backend - Test to confirm that the encryption is in place and is effective	1	4	4	Yes	Virtually impossible to intercept data if these controls are implemented.

11	Effectiveness in border areas where people live and work either side of borders could undermine effectiveness and thus justification of data processing proposed	- Ensure that the app is to augment the existing contact tracing and testing operations in Ireland and that under this umbrella, of wider operational cooperation and coordination, that app interoperability is considered. - Engaging the same developer as used by ROI in developing its app has helped two ensure that the two apps will be interoperable - Assurance testing will confirm this - Engage with Google and Apple in relation to cross border interoperability - Engage at an EU level in regards cross border interoperability	3	2	6	Yes	Through a commitment of ongoing engagement and exploration of coordination and cooperation possibilities with other countries, and the implementation of the mitigation measures, this risk is seen as significantly reduced.
12	Risk that bundling of related features in the pandemic response app infringes on the data protection principle of data minimisation	- Ensure the guidelines from the EDPB are carefully assessed - Ensure that features are clearly aligned with the purpose of the app being a COVID-19 response app - Ensure the Terms of the Governance Committee charge the committee with the above obligations - Engage the scientific community to independently assess the HCI and ethics aspect of the app to inform decisions - Data geolocked to datacentres in Europe (GDPR compliant).	2	2	4	Yes	Implementation of all mitigation measures will ensure that people can choose how their data is processed by selectively using or not the individual features within the app. There remains a small risk that users may not be aware of these options and careful and ongoing review of user experience is required.
13	The use of analytic data gathered from the device for the purposes of how the users interact with the app, daily use, app abandonment, contacts, exposure events, etc., is not anonymous and unexpected to the users. Risk to users that data is not anonymous.	- All metric data must be anonymised (or anonymised at the earliest processing point - noting IP address as per DPIA) and carefully reviewed for any re-identification potential - Release source code to ensure transparency of processing - Ensure app does not use 3rd party analytics tools to gather metric data, which could unintentionally or otherwise be recombined to re-identify people - Ensure app governance appropriately reviews and protects against this as per above	1	1	1	Yes	The risk has been mitigated as far as possible by anonymising the personal data so that there is little risk to the data subjects of their data becoming identifiable or useable in profile building or similar activities.

14	Users are not given sufficient information about how the app works, what data will be collected and for what purpose in a comprehensive way	- Careful consideration of UI/UX in regards information in the app screens informing people about what the app does - Engage in behavioural research to gain direct feedback on effectiveness of in app information - Data protection information notice (DPIN) - available in the app at all appropriate screens (all consent screens) and in settings at all times, in app stores, and DoH websites - Implement a communications plan to inform people about the app, what it does and what data is processed	1	1	1	Yes	Correct implementation of all mitigations leaves little risk to data subjects
15	Risk that Contact Tracing can be used to identify and track people's location and for profiling purposes, rather than tracking the virus	- Adopt a decentralised approach for the Contact Tracing function - Do not use location services for Contact Tracing - Adopt the Google and Apple API implementation, which is receiving significant worldwide analysis from privacy experts - Open source code for inspection - Do not pass IP addresses from networking layer to application layer in app backend to protect against re-identification potential - Implement security testing and assessment of app in this regard	2	3	6	Yes	After mitigation measures are implemented little likelihood remains
16	As the app knows when a person is uploading their diagnosis keys, risk the app can be used to display the COVID-19 status of a person and be used outside of its purpose	- The app will be designed to not show the COVID-19 status of a person - The independent oversight committee will oversee the app processes data in line with its purposes and the DPIA	1	1	1	Yes	With mitigation implemented there is minimal risk

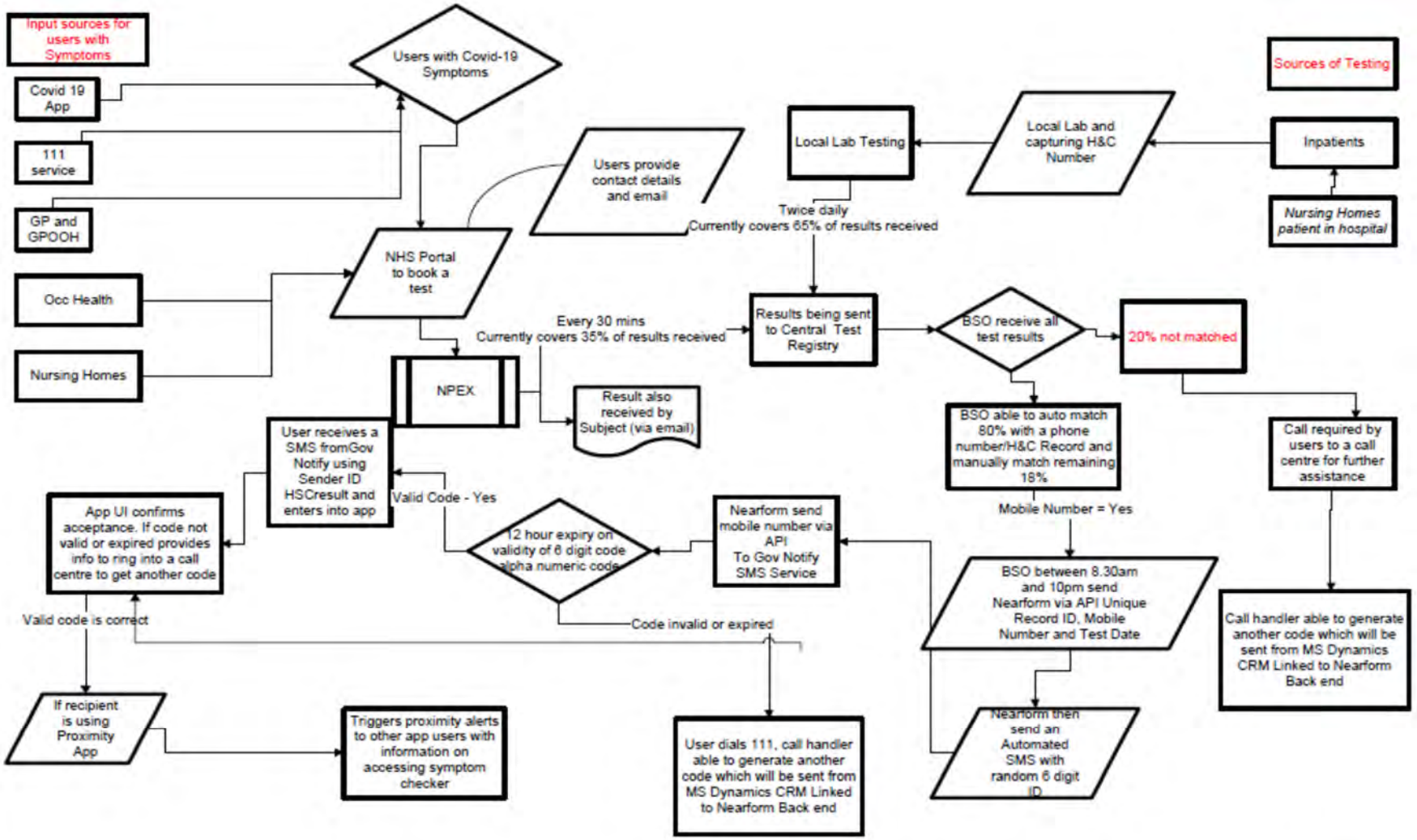
17	The use of the app may continue indefinitely or longer than justified by the defined purposes	- European Data Protection Guidelines state that contact tracing apps should remain active only for the period of the COVID-19 crisis, and as such this will be adhered to. - Terms of reference to charge oversight Committee to implement an orderly wind down of processing of personal data within 90 days of the COVID-19 crisis ending (declared by Government) - Introduce measures through the app and communications to prompt user action as appropriate as part of any wind-down	1	1	1	Yes	Little risk remaining to data subjects if all measures are implemented
18	IP address is present in all data transfers from the app to the app backend	- The app backend will not processing IP addresses at the application layer. This means no IP address leaves the network layer on the backend. - All app backend logging does not log user IP address	1	1	1	Yes	IP address does not leave app backend network layer and as such DoH cannot recombine with payloads to identify data subjects
19	The risk that SMS code provider can identify that particular person with particular notifications and then infer the COVID-19 positive status of the device owner	- The SMS delivery service Is provided by Gov.UK Notify, with the BSO providing support. There is separation of people and infrastructure with regards the app backend and the SMS server and 'test registry' functions; to prevent re-identification of data protecting confidentiality, and thus protect data subjects - use of a known and trusted SMS provider for this service mitigates risk	1	3	3	Yes	After mitigation it is unlikely to occur
20	Technical issues with the app that would reduce function or interfere in a negative way in the working of the other phone's function, thus reducing user engagement, lessening the app's effectiveness, and weakening the case for data being processed.	- App to be tested for impacts on other phone functions such as battery life, interference with Bluetooth peripherals, etc. - Use Apple and Google ENS to benefit from their ability to optimise functioning of the exposure notification service beyond what any app developer can	2	2	4	Yes	The mitigations will go some way to reducing the risk however the residual risks will not be known until app is fully tested

21	Role of Apple and Google may process data in a non-privacy enhancing way in the future, or in a way that is not desirable in respect of the rights of data subjects, that is unexpected	- Continually monitor and engage with Apple and Google to understand their plans and feedback regarding Ireland's requirements - Continually review plans and how data is processed and implement an exit from reliance on Exposure Notification Services if it falls out of line with GDPR - Work with other countries to engage with Google and Apple, and to collectively monitor the performance and behaviour of ENS	1	2	2	Yes	With mitigations implemented it leaves little net risk.
22	Integrity of data is compromised. The diagnosis keys, or mobile number uploaded to BSO servers is erroneous or corrupted, meaning it is unusable or unreliable.	- App and related technology infrastructure to undergone extensive information security testing to identify and rectify any issues. - All traffic in transit is encrypted - Certificate pinning and other security mechanisms are implemented to protect against 'man in the middle' attacks	1	4	4	Yes	The proposed risk treatments should largely remove risks to data integrity.
23	Users may decide to turn off the Bluetooth service on their phones for battery life or other reasons.	- Integrate into communications and within the app a clear message so people understand the impact of turning off Bluetooth on their phone - Clearly show, if people go into the app, that the Contact Tracing function is turned off (must respect consent)	2	3	6	Yes	It is difficult to ensure that users never turn off Bluetooth.
24	Continually downloading Diagnosis Keys may consume a user's network data allowance.	- Use a design that minimises the size of data downloads required - current estimates for Ireland and ENS is ~1MB per week downloaded. The amount of traffic sent to and from the device should not use up any significant portion of the user's monthly allowance or credit.	1	2	2	Yes	The residual risk would be one relating to the number of infections that would cause a jump in traffic
25	Users can't exercise their data protection rights or don't know where to go to exercise them.	- Provision of a DPIA and Privacy Notice to ensure it is clear to data subjects what rights they have, how to exercise them and with whom. - Ensure access to Privacy Notice and Terms & Conditions at all times via the app, and app related website - Implement a decentralised model for exposure notification to ensure limited personal data processed on app backend - Symptom data collected to be anonymous	1	1	1	Yes	There is only a small risk of this occurring based implementation of mitigation measures

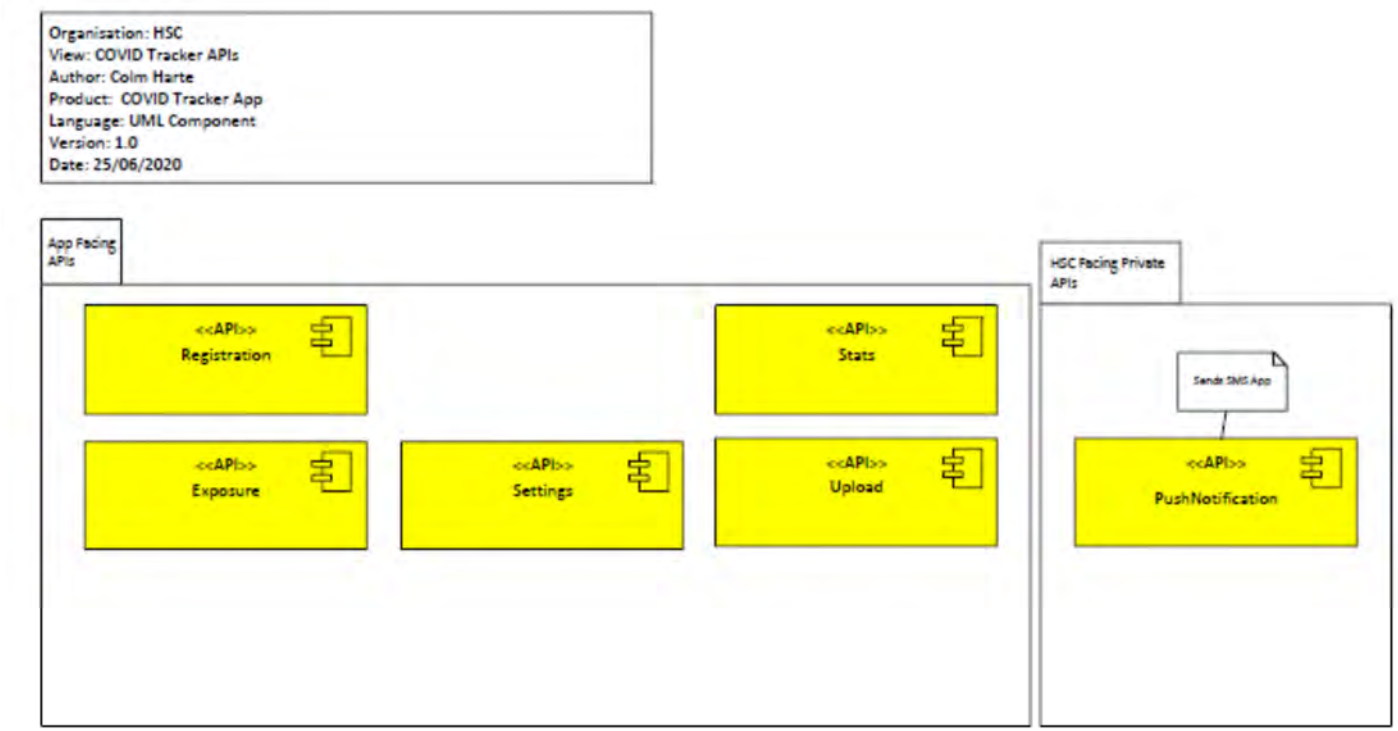
26	Failure to separate the backend architecture and support staffing could compromise anonymity allowing 're-identification' of data	-To prevent re-identification of users at the contact tracing server side it is important that the OTC generation and transmission are kept separate from the upload of TEKs. To facilitate this a separated approach has been taken to how these two flows operate. The OTC service and the upload service run in separate Fargate clusters to manage traffic segregation. -The mobile number used for SMS is not logged by the OTC service which utilises the Gov.uk Notify service for the SMS sending. This service is completely separate from the contact tracing app infrastructure. -Reconciliation between OTC requests and SMS messages sent will rely on comparing the log data from Gov.uk Notify with the request generated from the test registry. -The flow of data from the BSO test registry through the app backend to the Gov Notify (SMS Platform) to send an SMS will be managed by different groups to help reduce any risk of re identification.	1	1	1	Yes	With the outlined measures implemented, the risk is low
27	SMS messaging failure could be missed by the system, due to separation of teams, meaning that app users don't have a code to put into the app when they test positive	-The flow of data from the BSO test registry through the app backend to the Gov Notify (SMS Platform) to send an SMS will be managed by different groups to help reduce any risk of re identification. •The BSO registry contains the mobile numbers of people who have tested positive. • As the Temporary Exposure Key uploads hit the app backend in Amazon Web Services, it is important this backend data cannot be combined with mobile numbers. • To help prevent this the Amazon Web Services backend will never store or log the mobile number. • The mobile number will exist in the BSO test registry and will exist in Gov Notify as SMS messages are sent. -To facilitate reconciliation for issues that may occur within the Amazon Web Services backend, a Job ID will be used to track the flow from BSO registry through Amazon Web Services. When BSO calls the Amazon Web Services REST API it will pass on a Job ID that will be used to uniquely identify the transaction with the	1	1	1	Yes	With the outlined measures implemented, the risk is low

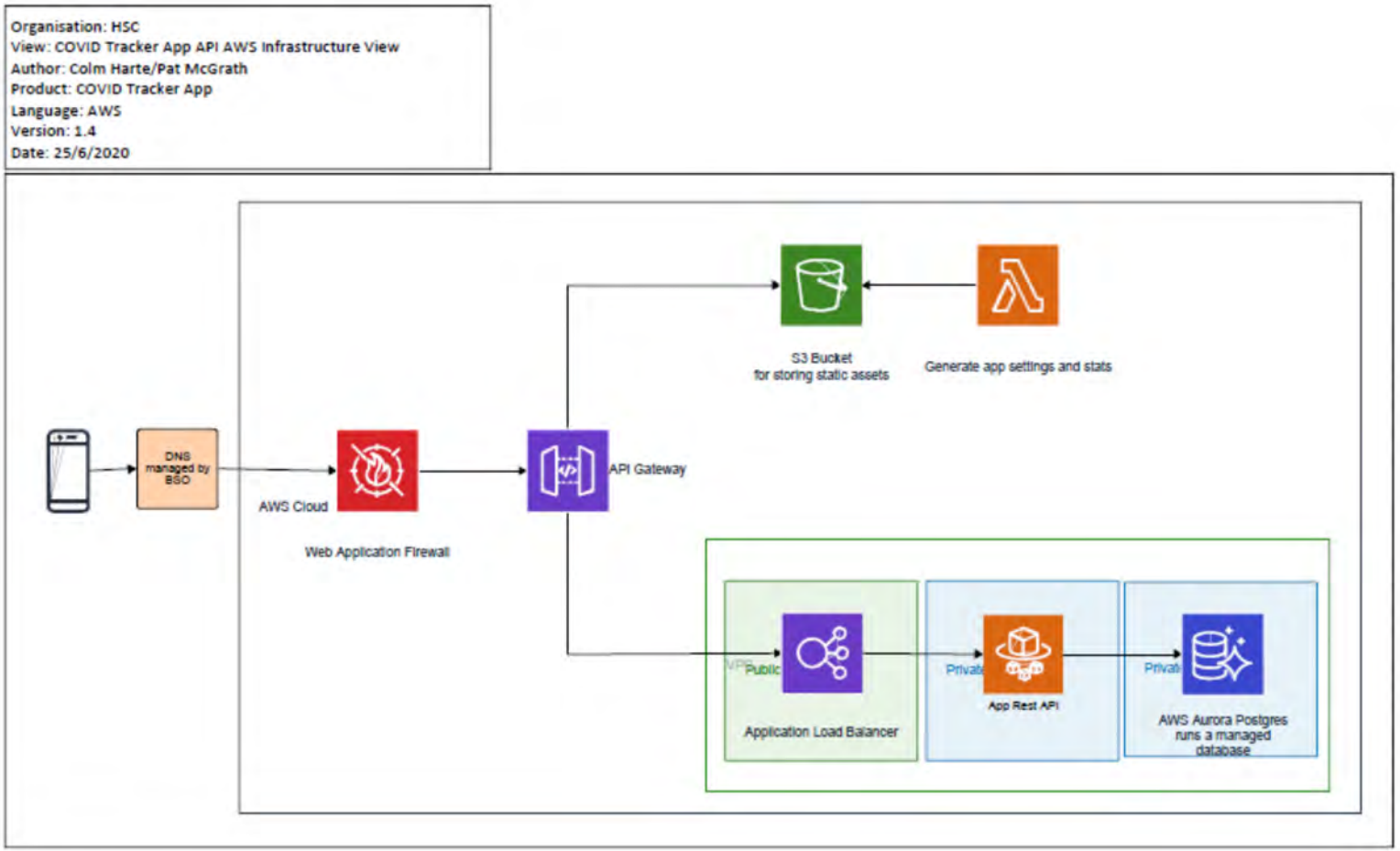
		Amazon Web Services flow. This Job ID will be logged within Amazon Web Services so that in the case of any failure during processing, the record in the BSO registry that was not successfully processed, can be identified. In the case of a failure during the Amazon Web Services flow, an alert will be raised within Amazon Web Services and notified to the NearForm support team. The Nearform team will investigate alerts raised and will either address and correct if the issue is within Amazon Web Services. If the issue is outside of Amazon Web Services then when appropriate NearForm will escalate the issue to the BSO support team. BSO will be required to reconcile the Job ID from registry data to the SMS records on the Gov Notify platform.					

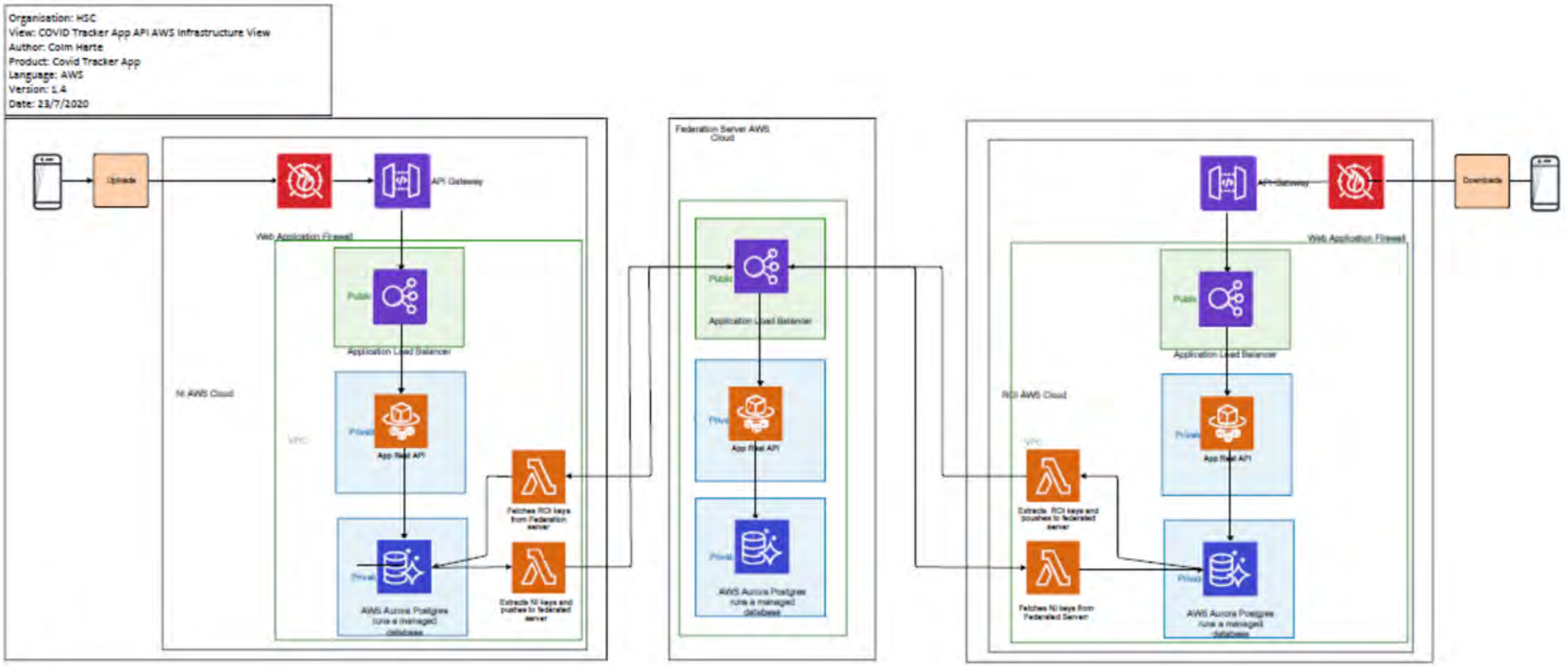
Appendix H – App Supporting Infrastructure and Data Flows

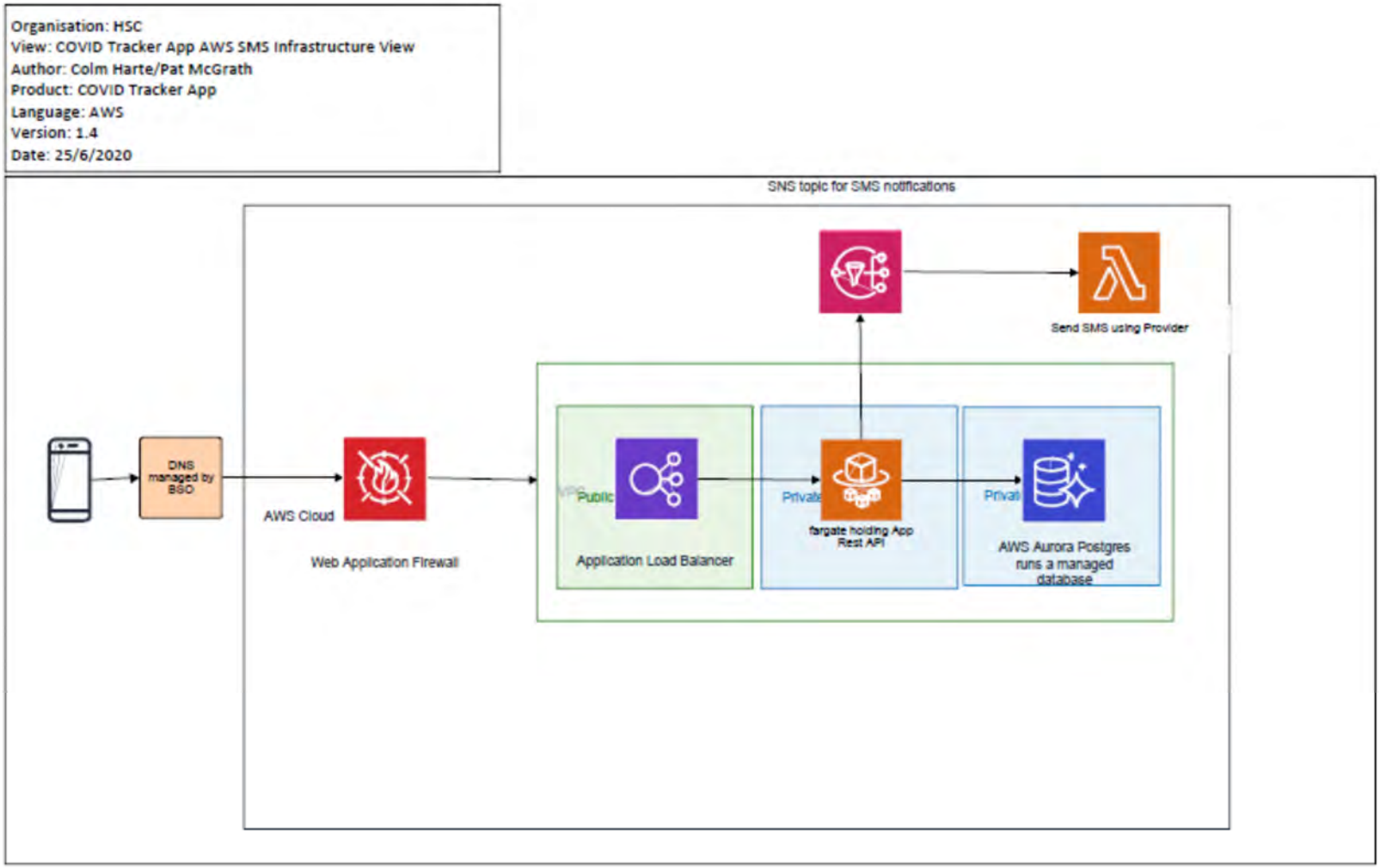


Flow for Contact Tracing
AppV0.4 24th July 2020

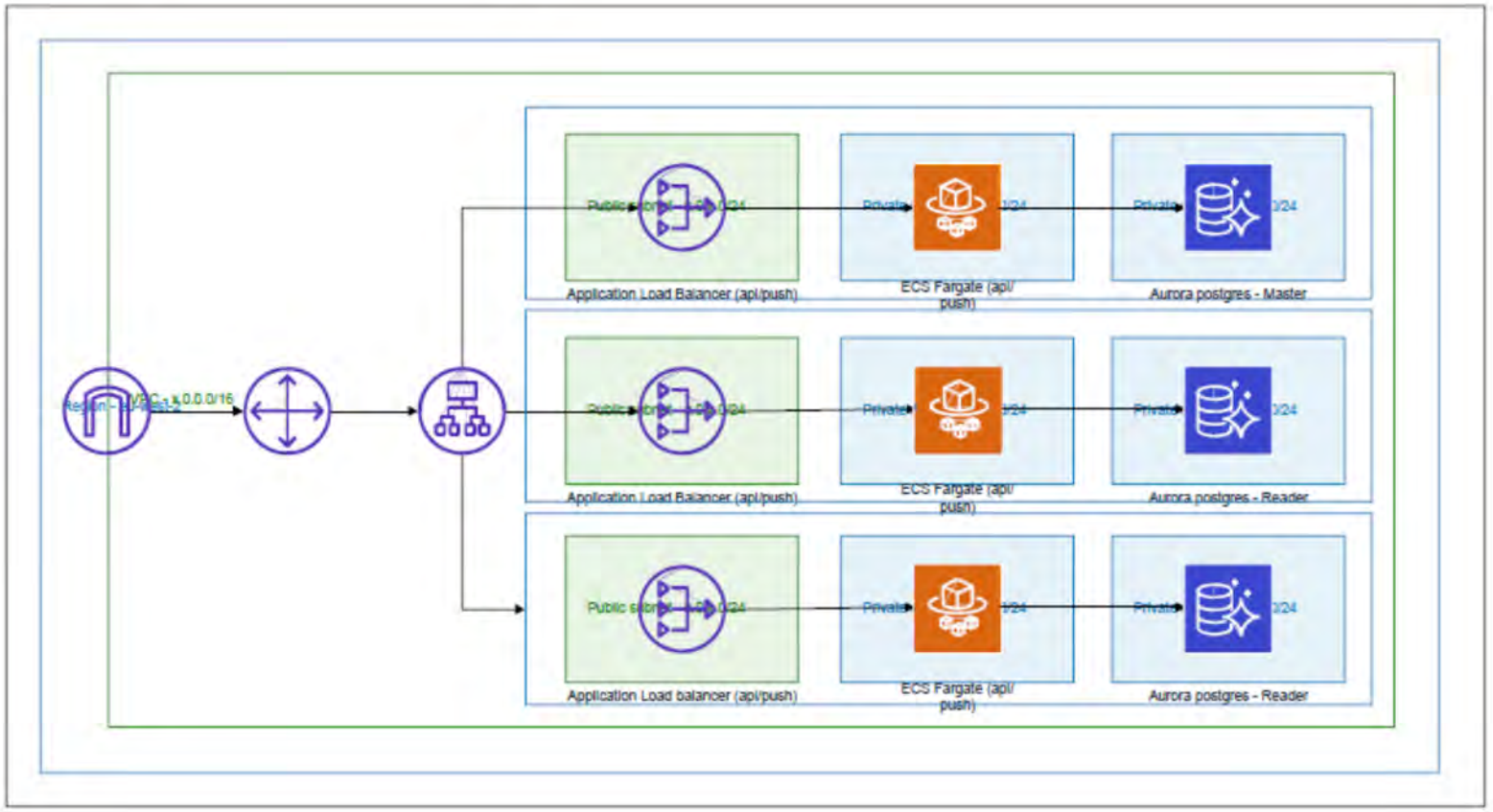

Organisation: HSC
View: COVID Tracker APIs
Author: Colm Harte
Product: COVID Tracker App
Language: UML Component
Version: 1.0
Date: 25/06/2020
App Facing APIs
<<API>>
Registration
<<API>>
Stats
<<API>>
Exposure
<<API>>
Settings
<<API>>
Upload
HSC Facing Private APIs
Sends SMS App
<<API>>
PushNotification

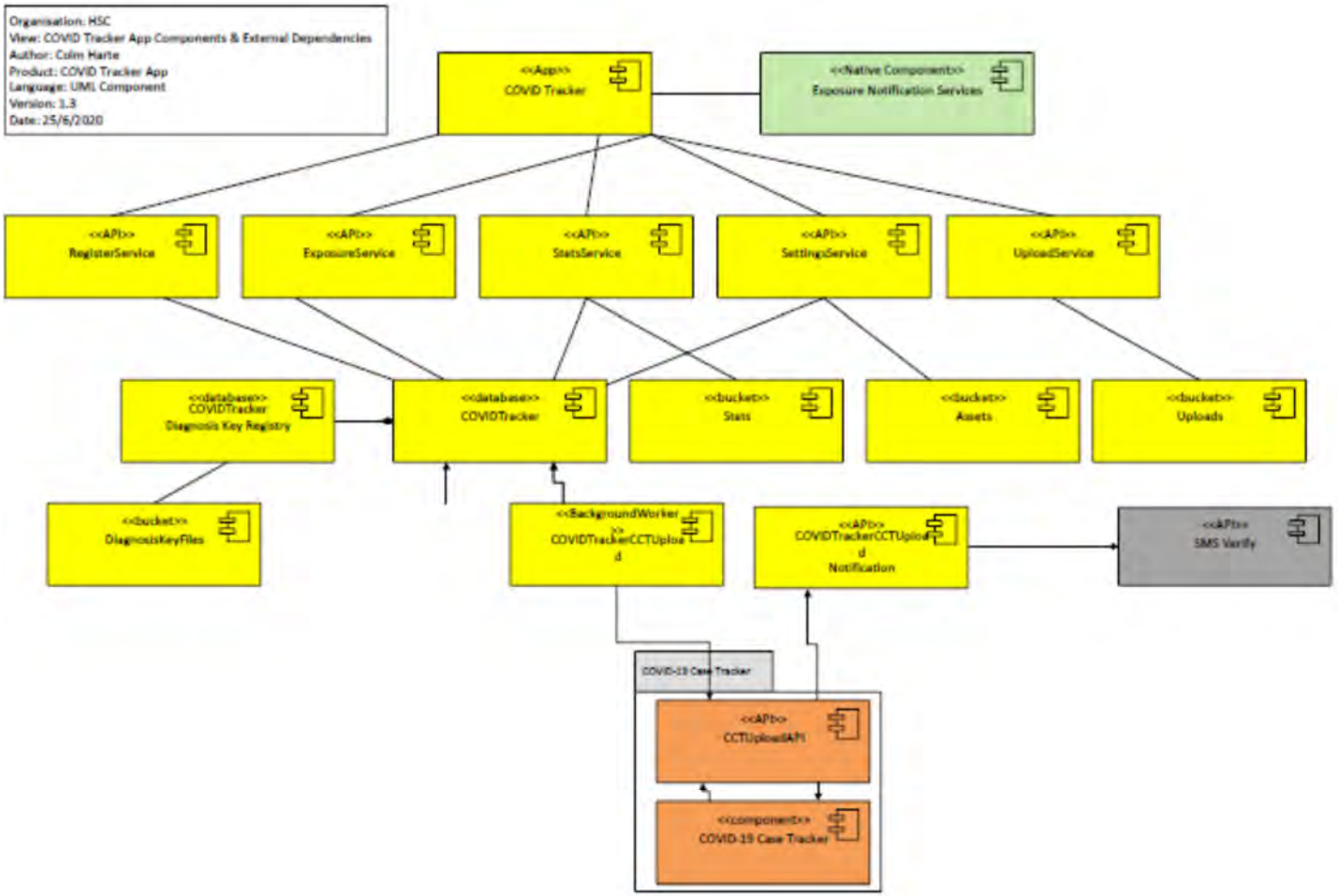

Organisation: HSC
View: COVID Tracker App API AWS Infrastructure View
Author: Colm Harte/Pat McGrath
Product: COVID Tracker App
Language: AWS
Version: 1.4
Date: 25/6/2020
S3 Bucket
for storing static assets
Generate app settings and stats
DNS
managed by
BSO
AWS Cloud
Web Application Firewall
API Gateway
Public
Application Load Balancer
App Rest API
AWS Aurora Postgres
runs a managed
database

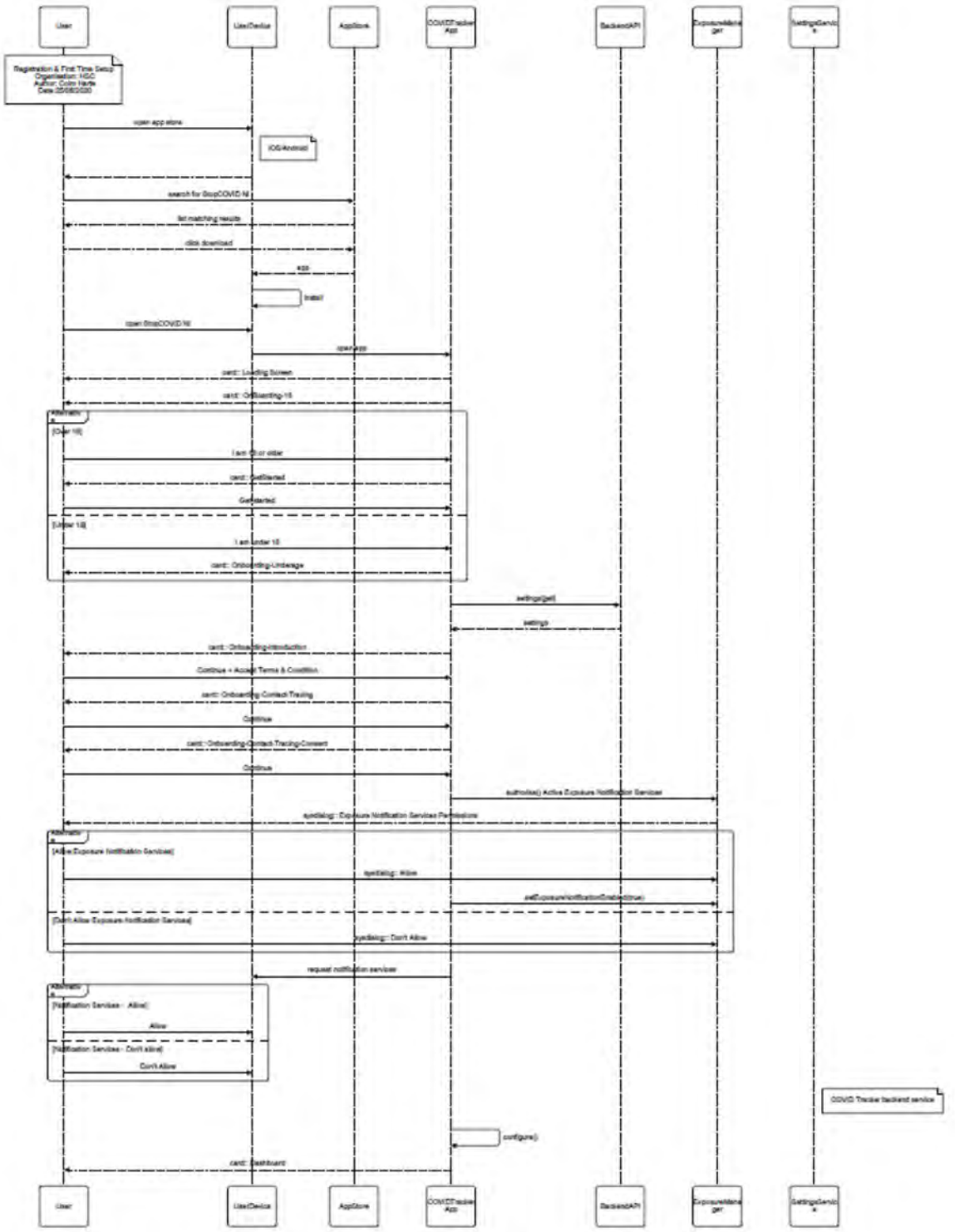

Organisation: HSC
View: COVID Tracker App API AWS Infrastructure View
Author: Colm Harte
Product: Covid Tracker App
Language: AWS
Version: 1.4
Date: 23/7/2020
Uploads
API Gateway
Web Application Firewall
Public
Application Load Balancer
NI AWS Cloud
VPC
Private
App Rest API
AWS Aurora Postgres (runs a managed database)
Fetches ROI keys from Federation server
Extracts NI keys and pushes to federated server
Federation Server AWS Cloud
ROI AWS Cloud
Extracts ROI keys and pushes to federated server
Fetches NI keys from Federated Server
Downloads

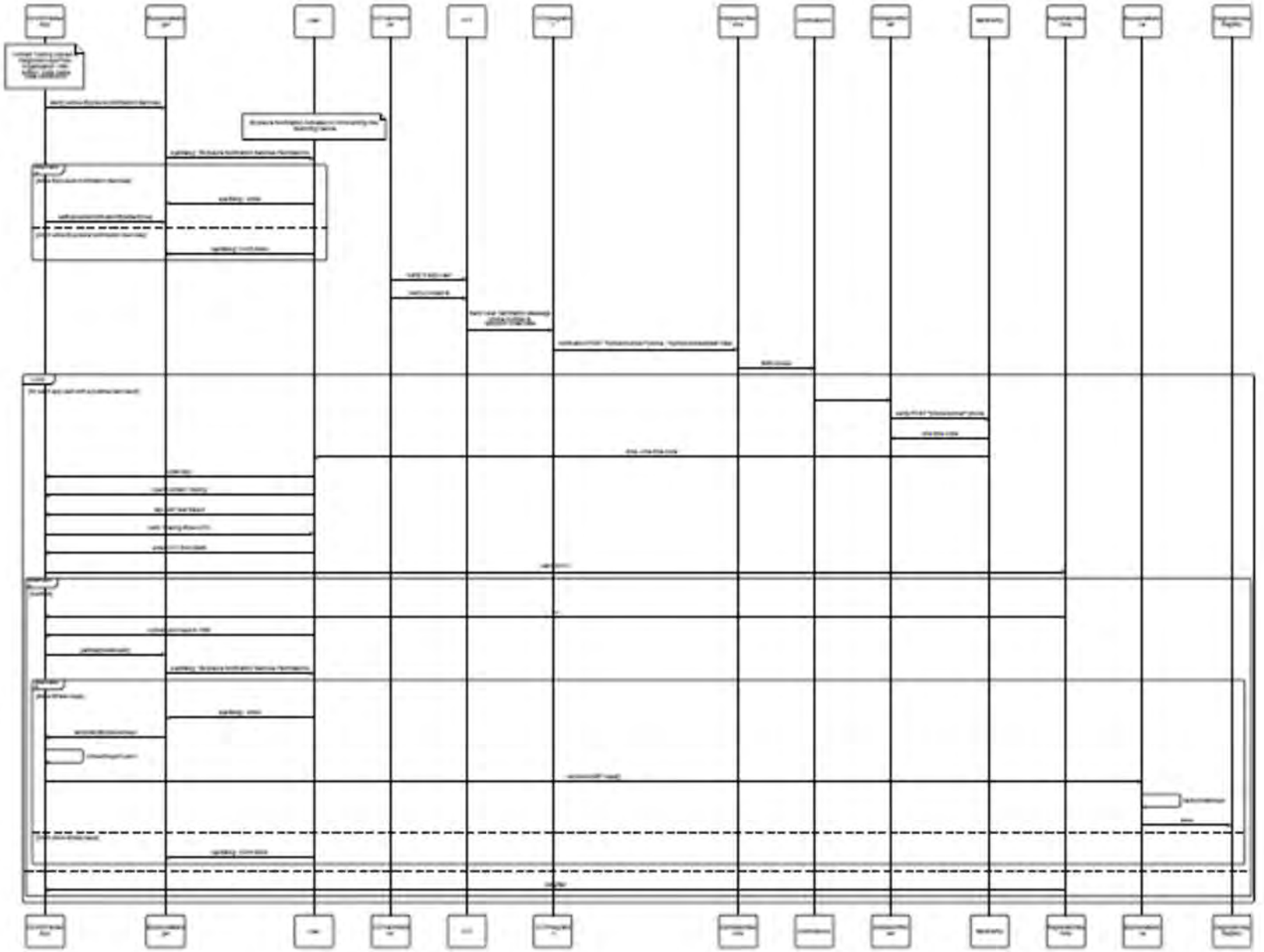

Organisation: HSC
View: COVID Tracker App AWS SMS Infrastructure View
Author: Colm Harte/Pat McGrath
Product: COVID Tracker App
Language: AWS
Version: 1.4
Date: 25/6/2020
SNS topic for SMS notifications
Send SMS using Provider
DNS managed by BSO
AWS Cloud
Web Application Firewall
Public
Application Load Balancer
Private
fargate holding App Rest API
Private
AWS Aurora Postgres runs a managed database

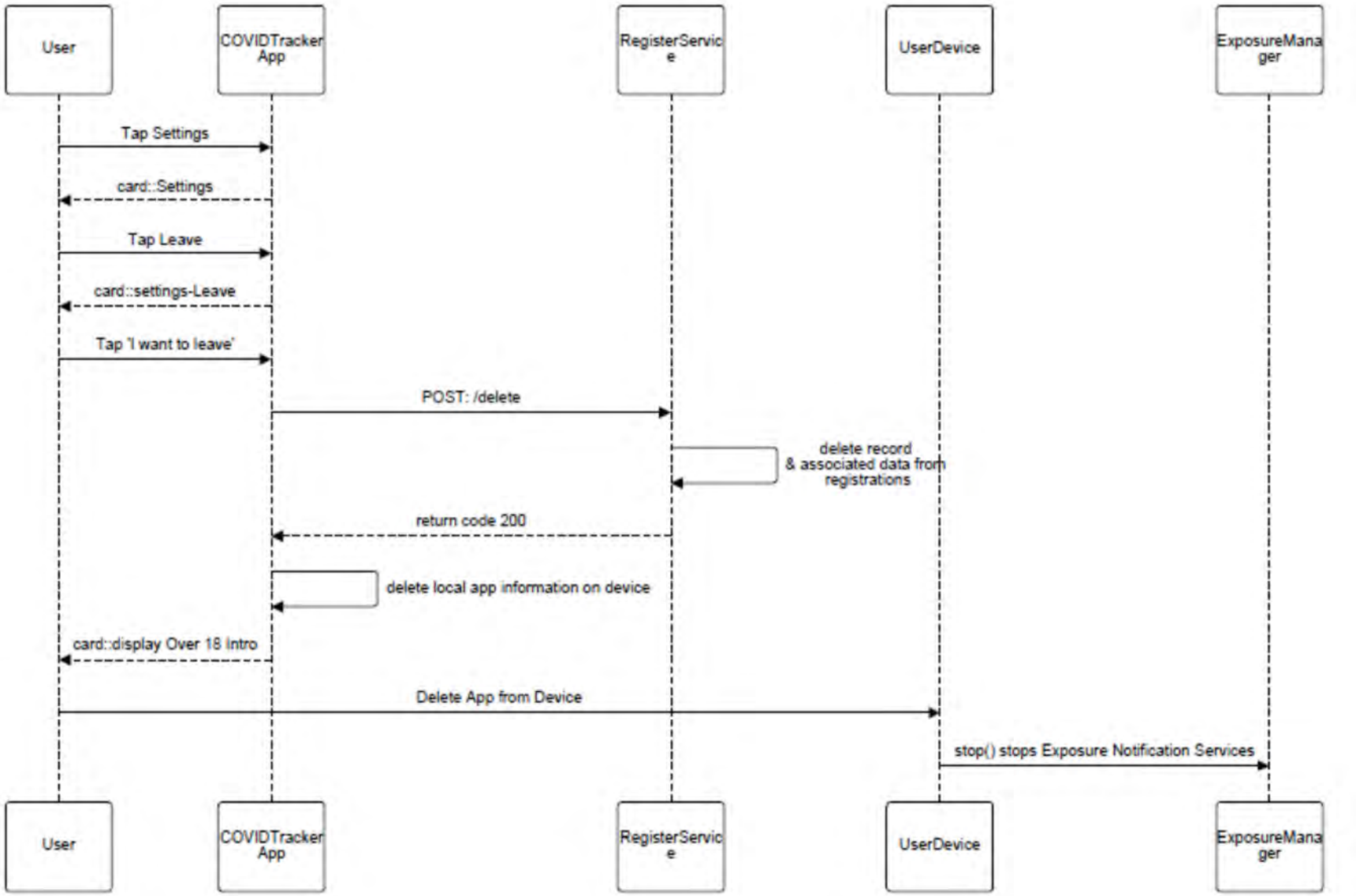
Organisation: HSC
View: COVID Tracker App AWS Network Configuration View
Author: Colm Harte/Pat McGrath
Product: COVID Tracker App
Language: AWS
Version: 1.4
Date: 25/6/2020

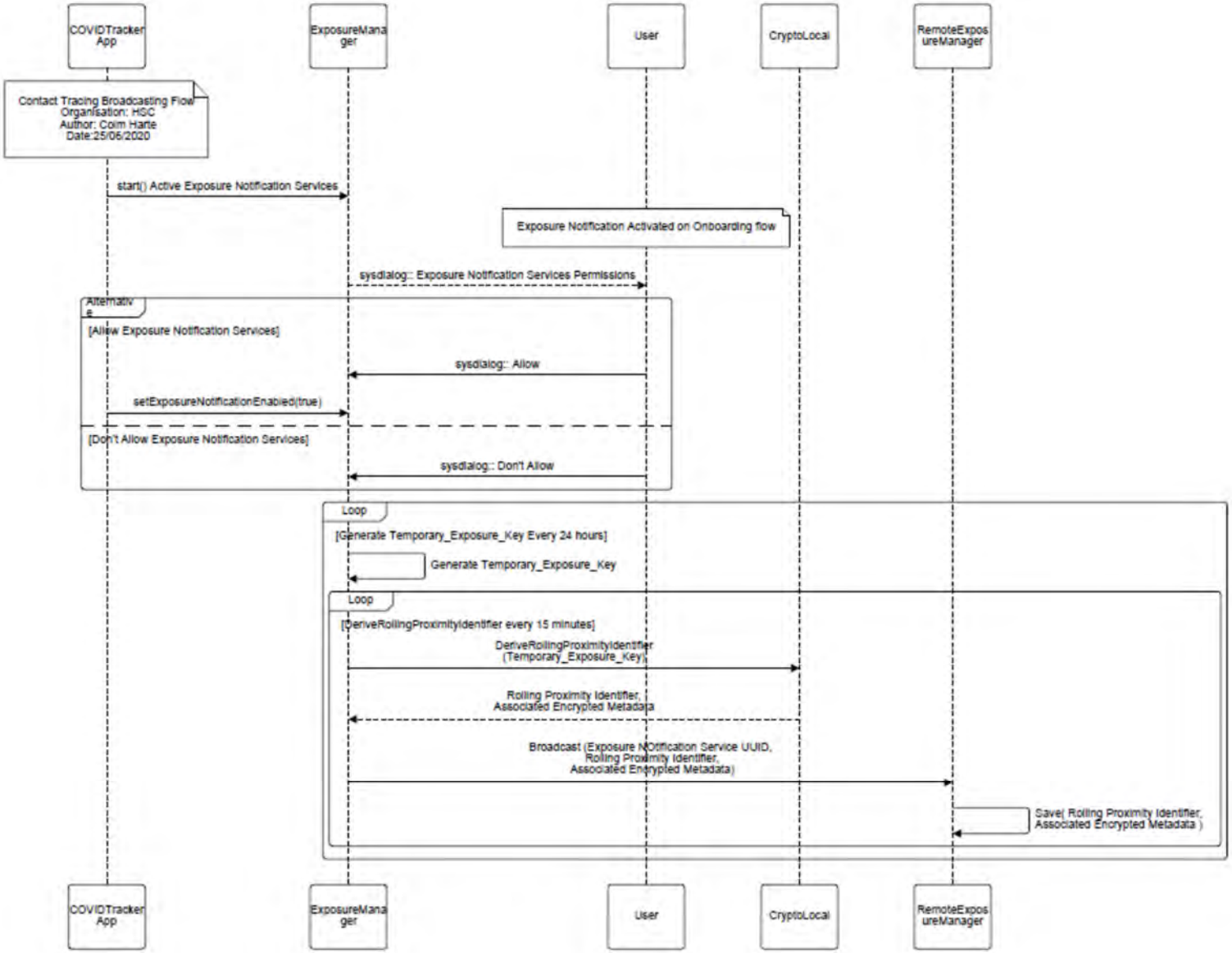


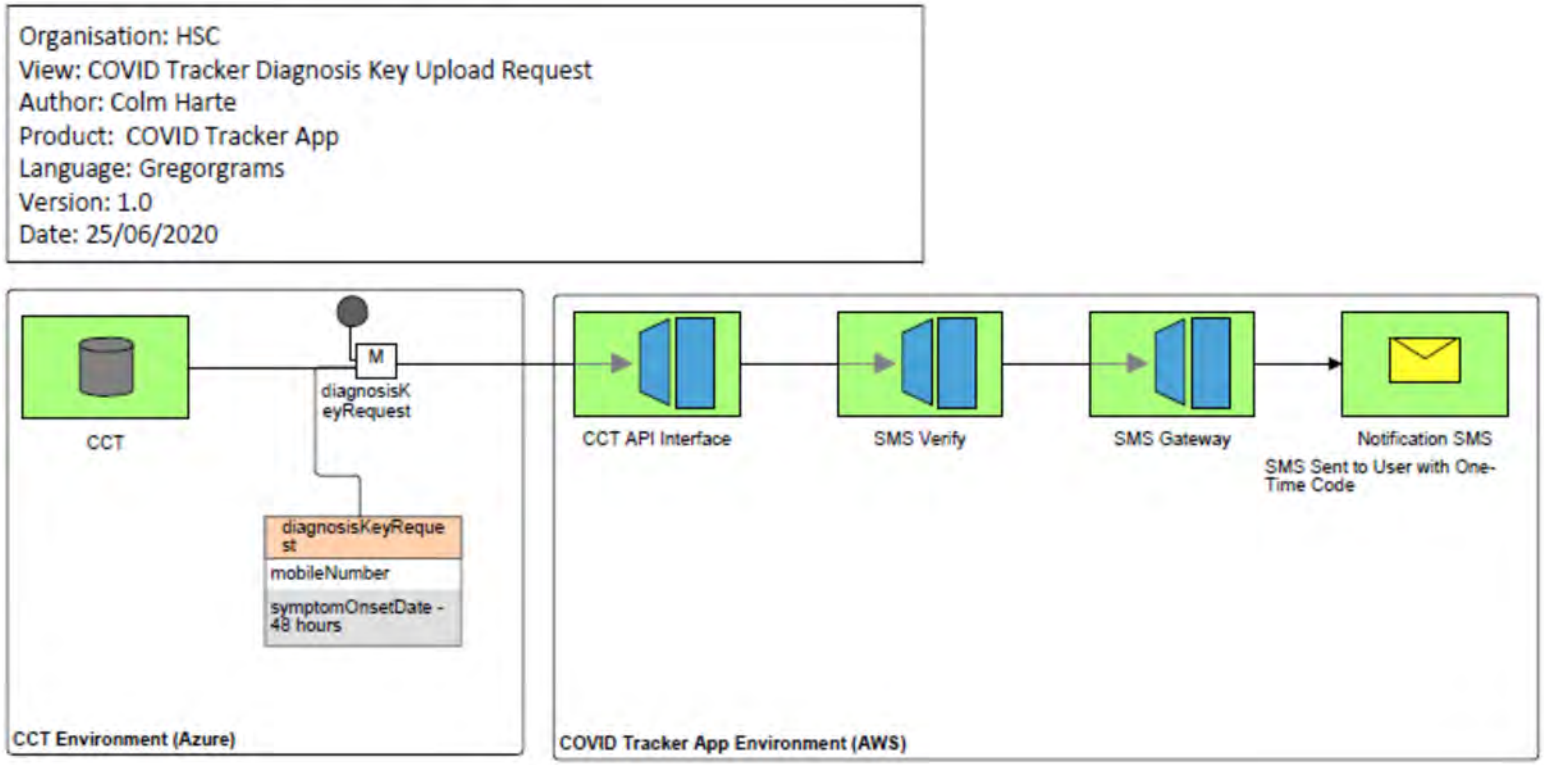

Organisation: HSC
View: COVID Tracker App Components & External Dependencies
Author: Colm Harte
Product: COVID Tracker App
Language: UML Component
Version: 1.3
Date: 25/6/2020
<<App>>
COVID Tracker
<<Native Component>>
Exposure Notification Services
<<API>>
RegisterService
<<API>>
ExposureService
<<API>>
StatsService
<<API>>
SettingsService
<<API>>
UploadService
<<database>>
COVIDTracker
Diagnosis Key Registry
<<database>>
COVIDTracker
<<bucket>>
Stats
<<bucket>>
Assets
<<bucket>>
Uploads
<<bucket>>
DiagnosisKeyFiles
<<BackgroundWorker
>>
COVIDTrackerCCTUploa
d
<<API>>
COVIDTrackerCCTUploa
d
Notification
<<API>>
SMS Verify
COVID-19 Case Tracker
<<API>>
CCTUploadAPI
<<component>>
COVID-19 Case Tracker

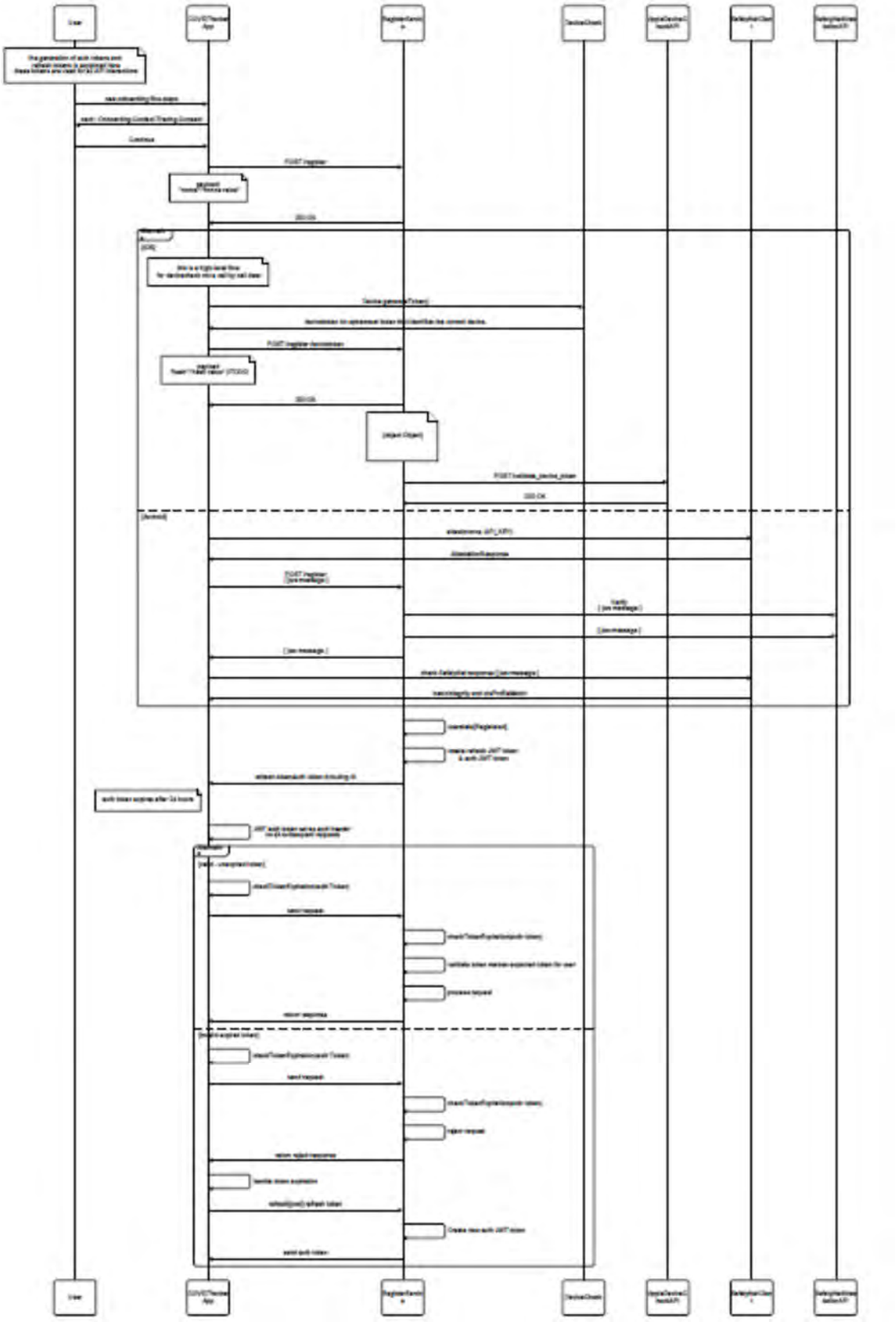





User
COVIDTracker App
RegisterServic e
UserDevice
ExposureMana ger
Tap Settings
card::Settings
Tap Leave
card::settings-Leave
Tap 'I want to leave'
POST: /delete
delete record & associated data from registrations
return code 200
delete local app information on device
card::display Over 18 Intro
Delete App from Device
stop() stops Exposure Notification Services
User
COVIDTracker App
RegisterServic e
UserDevice
ExposureMana ger


COVIDTracker App
ExposureManager
User
CryptoLocal
RemoteExposureManager
Contact Tracing Broadcasting Flow
Organisation: HSC
Author: Coim Harte
Date:25/06/2020
start() Active Exposure Notification Services
Exposure Notification Activated on Onboarding flow
sysdialog:: Exposure Notification Services Permissions
Alternative
[Allow Exposure Notification Services]
sysdialog:: Allow
setExposureNotificationEnabled(true)
[Don't Allow Exposure Notification Services]
sysdialog:: Don't Allow
Loop
[Generate Temporary_Exposure_Key Every 24 hours]
Generate Temporary_Exposure_Key
Loop
[DeriveRollingProximityIdentifier every 15 minutes]
DeriveRollingProximityIdentifier (Temporary_Exposure_Key)
Rolling Proximity Identifier, Associated Encrypted Metadata
Broadcast (Exposure Notification Service UUID, Rolling Proximity Identifier, Associated Encrypted Metadata)
Save(Rolling Proximity Identifier, Associated Encrypted Metadata)
COVIDTracker App
ExposureManager
User
CryptoLocal
RemoteExposureManager


Organisation: HSC
View: COVID Tracker Diagnosis Key Upload Request
Author: Colm Harte
Product: COVID Tracker App
Language: Gregorgrams
Version: 1.0
Date: 25/06/2020
CCT
M
diagnosisKeyRequest
diagnosisKeyRequest
mobileNumber
symptomOnsetDate - 48 hours
CCT Environment (Azure)
CCT API Interface
SMS Verify
SMS Gateway
Notification SMS
SMS Sent to User with One-Time Code
COVID Tracker App Environment (AWS)



Appendix I –Support Function: Preventing Re-identification of Data

1. The format of the data from the BSO to Nearform will include a Unique Record ID, Date of Test and Mobile Number to be sent to Nearform via API from 08.30 to 21:30 (hourly)

- BSO and Nearform will actively monitor both sides of the API and liaise to resolve

2. Nearform will provide support and active monitoring of the API to BSO and also the Amazon Web Services (AWS) backend where the App is hosted and also the API to the Gov Notify SMS platform.

3. The Supervisor in the Manual Contact Tracing Centre will have access to the SMS Platform (Gov Notify) and also the Dashboard to check delivery status of SMS messages.

4. The Manual Contact Tracing Centre will also be the point of contact to the Gov Notify SMS service status via email for Service Outages https://status.notifications.service.gov.uk/ and will also be able to log support calls via the Gov Notify support portal https://www.notifications.service.gov.uk/support

Appendix J – Privacy Notice

Privacy Information

Data Controller Contact Details

Department of Health (DoH)
Castle Buildings
Stormont
Belfast
BT4 3SG

Contact- Chief Digital Information Officer Group

CDIO@health-ni.gov.uk

Data Protection Officer

Charlene McQuillan

DPO@health-ni.gov.uk

Introduction

The purpose of this information notice is to explain how the StopCOVID NI Contact Tracing App works, what data is collected by the app, and who has access to that data and the purposes for which they use it.

Use of the app is entirely voluntary and is available to download for free from the Apple App Store and the Google Play Store. The app runs on iPhones that support iOS 13.5 and higher, and Android phones running Android 6.0 and higher. The App is not intended for use by persons under 18 years of age, at present, as anonymity to protect App users (in line with GDPR) creates a conflict with safeguarding issues, and the requirement for parental consent. You will be asked to confirm that you are 18 years or older when you download the App. The App is only intended for use by individuals resident in Northern Ireland. You will be asked to confirm residency and will be discouraged from using the App if you do not meet this criteria. We accept no liability for improper use, outside these defined conditions.

The Data Controller

The Department of Health (DoH) in Northern Ireland is the Data Controller – it has decided the means and purposes for the processing of data collected and used by the app. The DoH, working with the Health and Social Care Board and Public Health Agency (PHA), has commissioned all app related systems for processing all data. The DoH provides strategic direction for the app.

The DoH is therefore responsible for your personal data and has determined its responsibilities for compliance with its obligations under data protection laws. The DoH has provided access to speak to someone via '0300 200 7896' Monday-Friday (excluding bank holidays) between the hours of 8:30am – 5:30 pm, should you wish to raise an issue in relation to how your data is managed by the App, though note that you also have the right to contact the Data Protection Officer in this regard.

Version 6.0. 31st July 2020

What the app does

The purpose of the app is to support the public health response to the COVID-19 crisis in Northern Ireland. The app has the following functions:

1. Exposure Notification – the App, through use of anonymous 'keys', records when App users' phones have been in proximity to each other, for a sufficient period of time to mean that it is possible that the coronavirus has been passed on. Should an App user test positive for COVID-19, it is possible for them to alert other App users anonymously via the functions supported by the App.
2. Registering a Positive Test Result – App users who have a positive test for COVID-19 will receive a randomly generated 'authorisation code' via SMS text message. This process is managed via a separate test registry, administered by the Regional Business Services Organisation (in accordance with its statutory functions as defined in the Health and Social Care (Reform) Act (Northern Ireland) 2009). This is separate from the App, in order to keep personal and identifiable information separate from the APP.
3. Other Functions – the app will collect Metric data which do not identify you in order to create aggregate views of how the App is being used and the impact it is having on controlling the spread of the virus. Here is a list of the App metrics which, are collected from your App. The collection of these metrics is essential in order to prove efficacy and gain CE accreditation:

    a. The total number of App users
    b. The total number of instances where 'diagnosis keys' have been uploaded
    c. The total number of 'exposure notifications' triggered

    The DoH will not know any of these instances related to any individual app user, simply total numbers (for the region) of 'authorisation codes' and 'exposure notifications' in any given time period. **As a precaution, in information governance terms, we treat the metrics as 'health data' to ensure your information is protected in terms of GDPR legislation.**

You are not requested to enter any personally identifiable information on the App. The 'App settings' give you the ability to delete the App and any information stored on the phone while using the App. The information collected is essential in allowing the App to meet its obligations for formal approval as a medical device and CE accreditation; in line with requirements published by the Regulator, MHRA. The regulator, in line with stated policy for the period of the COVID-19 pandemic, has granted a 6 month approval of the App for use, until formal permanent accreditation is obtained. Appropriate interim assurance on reliability and effectiveness has been provided to the regulator. Your explicit consent is obtained during the on-boarding process in order to enable the release of the diagnosis keys and to enable decisions to be taken on an automated basis. Collection of the metric data is essential for the DoH meet its regulated obligations in relation to CE accreditation, and to allow the DoH to support the essential public health function of contact tracing in delivering infection control measures in the context of the COVID-19 pandemic.

The phones of those who are using the App emit anonymised coded 'keys', 'Identifier Beacons', which change every 15 minutes. These 'keys' are stored on the user's phone for 14 days before being discarded. When close to each other, App users' phones exchange these anonymous 'keys', and if they are in close proximity with another user for a significant period of time (currently defined as 2 metres or less, and a duration of 15 minutes or more), both will store the anonymous 'key' of the other phone for 14 days.

'Authorisation Codes' are anonymous random six digit alphanumeric codes generated to verify that a positive test has been received by the App user, allowing 'exposure notifications' to be sent via the App, when the user enters a

valid 'authorisation code.' On entering the code, the user is asked to release the anonymous keys their phone has transmitted over the previous 14 days: these are then known as 'diagnosis keys'. These are then released to the secure registry, (see details below - HSCB AWS account), supporting users of the App, to be shared with other App users.

'Diagnosis keys' are anonymised identifiers generated on entry of an 'authorisation code' on the App, and stored in a secure registry, maintained in a Health & Social Care Board secure cloud services account (on behalf of the DoH) on Amazon Web Services (based in London). Every App user's phone regularly checks for 'diagnosis keys' and where these match a significant contact episode's anonymous 'key' stored on their phone, over the previous 14 days, an 'exposure notification' is enabled. The notification is generated on the App user's phone, not in the secure registry.

Where 'Exposure Notification' (ENS) is mentioned, this refers to an anonymous notification received, via the App, that you have been in contact with an unnamed individual who has tested positive for COVID-19, and that contact was recent enough, and for sufficient time, at a close enough distance to mean that you may have been infected.

The DoH is content to give a firm assurance that it has no intention to add to the functions of the StopCOVID NI App, beyond those identified above.

Future updates of the App may occur to improve the performance of existing functions, or to implement improvements in the Google-Apple operating system that may occur to improve performance, within the scope of existing functions (outlined above). The DoH is considering the future development of versions of the App, to address accessibility in terms of languages other than English. This decision will be balanced against public health benefit and cost (balanced against other health priorities).

How the app works

Let's look at each feature in the app in detail.

How Contact Tracing works

Existing manual contact tracing processes rely on you being able to remember who you have been in contact with recently, and for how long. In many cases you may not even know those people (for example, if the contact happened on a bus or train, at a concert, a restaurant or some other public venue).

The app uses technology developed by Apple and Google where anonymous rolling identifiers are exchanged between mobile phones. A random and unique identifier is generated by your phone every 15 minutes (range - 10 to 20 minutes). If you are close to someone, who also uses the app on their phone, your identifier will be saved on that person's phone and you will record their identifier on your phone. All identifiers collected will remain on your mobile but you can't see them, nor can anyone else. These anonymous identifiers cannot identify you, to other users, or to the DoH.

If a person using the App subsequently receives a positive COVID-19 diagnosis, they will receive a text message containing an 'authorisation code' via SMS. The Business Services Organisation test registry generates a test notification to all those who have a registered mobile phone number on their records, or who have registered for testing via the website https://www.nhs.uk/ask-for-a-coronavirus-test. The Business Services Organisation does not know who is using the App, so notifications are sent to in relation to all positive tests, where mobile phone numbers have been registered to testing services or for receipt of medical services in NI. All those with a positive

test will also receive a phone call from a clinical professional as part of the 'Test Trace and Protect' programme, administered by the Public Health Agency (PHA) under powers available through the 'Health and Social Care (Reform) Act (Northern Ireland) 2009'. On the call, they will be asked if they are using the StopCOVID NI Contact Tracing App and if yes, if they have not already done so, if they wish to enter an 'authorisation code' to the app to enable the upload of 'diagnosis keys' from their phone. To do this, the PHA will send them a code by SMS, which when entered into the app unlocks an upload function. The person makes a choice to upload 'authorisation code' and release 'diagnosis keys' relating to the anonymised identifiers of significant contacts processed on their own phone, to a secure registry maintained in a Health & Social Care Board secure cloud services account (on behalf of the DoH) on Amazon Web Services based in London; where the 'diagnosis key' identifiers are published to be visible to other App users phones, enabling 'Exposure Notifications'. The SMS text message is delivered using the Gov.UK Notify service https://www.notifications.service.gov.uk/ .

Every two hours, the latest 'Diagnosis Keys' from the App Registry will be downloaded by every user's phone. These will be used to check for matches against the identifiers of the contacts that have been collected by your phone. If there is a match, you will be notified in the app that you were in close contact with a person who was diagnosed with COVID-19; this is called an 'Exposure Notification'.

For all this to work, you have to allow 'COVID-19 Exposure Notification Services' on your phone. You can also choose to allow your phone to display notifications so that you also receive an alert on your phone that you have been exposed to someone who has tested positive for COVID-19. You can turn off this functionality, if you change your mind, in the settings page of the app.

It is important to note that Contact Tracing never reveals the identity of any person using the app to other app users, and never reveals who has been diagnosed positive. Also, the PHA and DoH will not know if you receive an 'exposure notification'.

Automated processing. The generation of exposure notices on the app is an automated process, not involving a human. The automated process is carried out by use of anonymous identification keys, and measurement of Bluetooth signals to calculate that App users' phones have been close enough for long enough to constitute a significant contact, sufficient to put you at risk of having been infected. It is necessary for the app to do this in an automated way, in order to protect your identity and the identity of other app users. In accepting terms and conditions you are consenting to this process. If you need to discuss this with an individual, you can call '**0300 200 7896**' Monday-Friday (excluding bank holidays) between the hours of 8:30am – 5:30 pm. **App users can express their point of view and contest the decision.**

What App metrics are collected

1. Collected regionally

The app will collect Metric data, which does not identify you, to create aggregate views of how the App is being used and the impact it is having on the control of the virus. Here is a list of the App metrics which, are collected from your App. The collection of these metrics is essential in order to prove efficacy and gain CE accreditation:

1. The total number of App users
2. The total number of instances where 'diagnosis keys' have been uploaded
3. The total number of 'exposure notifications' triggered

The DoH will not know any of these instances related to any individual app user, simply total numbers (for the region) of 'authorisation codes' and 'exposure notifications' in any given time period.

2. Generated by services on the phone

The following data is generated by Exposure Notification Services running on your phone if you turn it on.

1. Identifiers sent and received between phones that have ENS turned on.
2. Identifiers (diagnosis keys) uploaded to the Health & Social Care Board (HSCB) secure cloud services account (on behalf of the DoH) on Amazon Web Services (based in London) (AWS) Registry if you are COVID-19 positive and you agree to upload them.
3. Identifiers (diagnosis keys) downloaded from the AWS Registry to your phone for matching.

The above identifiers are random alpha numeric values that cannot be used to identify you or anyone else. These are generated, collected and matched on your phone if you enable ENS.

3. Automatically collected from your phone:

As a consequence of how traffic passes across the Internet, your internet protocol (IP) address is also inevitably transferred to our network servers. An IP address is typically made up of 4 sets of numbers (e.g. 1.2.3.4) and is assigned to you by your mobile phone or Wi-Fi service provider. Under the GDPR your IP address is regarded as your personal data.

While your data travels with the IP address it is considered personal data. The DoH does not use your IP address to identify you; furthermore the IP address is removed and deleted at the 'font door' of the HSCB AWS account, and the information becomes anonymous again and cannot be linked back to you. We do **not** store the IP addresses.

The legal basis for data processing

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 together form a framework for regulating the processing of personal data in the UK from 25th May 2018.

In relation to 'Metrics' and 'IP address and app security tokens' the '**processing is necessary for the performance of a task carried out in the public interest**' as per GDPR Article 6(1)(e). The legal basis for the data processing is The Health and Social Care (Reform) Act (Northern Ireland) 2009,

- Section 2(1) the duty to promote in Northern Ireland an integrated system of health care designed to secure improvement in the physical and mental health of people in Northern Ireland and in the prevention, diagnosis and treatment of illness, and
- Section 2(3)(g) the duty to secure the commissioning and development of programmes and initiatives conducive to the improvement of the health and social well-being of people in Northern Ireland, and
- Section 3(1)(b) the power to provide, or secure provision of, such health and social care as it considers appropriate for the purpose of discharging its duty under section 2; and do anything which is calculated to facilitate, or is conducive or incidental to, the discharge of that duty.

In relation to Special Category data, Article 9(2)(i) applies to the processing, '**processing is necessary for reasons of public interest in the area of public health**'. Under DPA 2018, Schedule 1, Part 1 condition 3 is met in relation to Article 9 as follows:

Public health

3 .This condition is met if the processing—

a) is necessary for reasons of public interest in the area of public health, and
b) is carried out—
    i. by or under the responsibility of a health professional, or
    ii. by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

The app cannot function beyond the initial 6 month MHRA Exemption from device regulation during COVID-19 without attaining CE accreditation. The metrics data, collected at a regional level, are essential in demonstrating efficacy (which will be essential for attaining accreditation). The app cannot be used beyond the 6 month exemption without accreditation. A mobile smartphone cannot link via a network to transfer data without use of an IP address and app security tokens. This information is deleted at the earliest opportunity and not stored anywhere in the infrastructure.

The MHRA guidance on medical devices states:

- "The software must meet all of the general essential requirements and the relevant design and construction essential requirements contained in 'annex I' of the directive. This guidance lists those essential requirements that are likely to apply to software and apps."

General Requirement 3 within Annex I of the Medical Devices Directive states:

- "The devices must achieve the performances intended by the manufacturer and be designed, manufactured and packaged in such a way that they are suitable for one or more of the functions referred to in Article 1(2)(a), as specified by the manufacturer."

'Diagnosis Keys' are released from the phone by the permission of the data subject. They are essential for letting others know that they are at risk of having been infected via the 'exposure notification' process. A person using the app may receive 'exposure notifications' by using the app, utilising the published 'diagnosis keys' of others. They may however decline to enter and 'authorisation code' on receipt of a positive test result, or may decline to release their 'diagnosis keys' for publication. While it is not anticipated that anyone would wish to use the app in such a manner, it is technically the position that release of 'diagnosis keys' is not essential for an app user to consent to this publication process, in order for them to benefit from notification by others. Technically it is arguable that at the point where 'diagnosis keys' exit a user's phone, they are associated with an IP address and app security tokens, and as such are personally identifiable. Though IP addresses vary, and are not static, some more recent rulings have deemed them 'personally identifiable'. Once the IP address and app security tokens have been deleted on entry to the networking layer, the 'diagnosis keys' are non-identifiable. Once stored in the app registry, the 'diagnosis keys' are clearly non-identifiable, and can be published without risk of re-identification. The app is voluntary to use and the legal basis for the processing of the 'diagnosis keys' is 'consent', namely GDPR 6(1) (a), and GDPR 9(2) (a), explicit consent, in relation to the processing of special category data. Consent is sought for release of the 'diagnosis keys' on the app at the point of release.

Security measures

All data stored on your phone is encrypted by the app using the built-in encryption capability of your phone. Data is also encrypted when it is being uploaded to our servers. The App does not store or transmit identifiable information. The App **does not access** GPS functionality on the phone, or access any form of location data from the operating system.

The Contact Tracing feature uses a **fully decentralised** privacy model which means that the matching of identifiers and diagnosis keys happens on your phone and is not externally performed by the DoH. This ensures neither tracking of peoples' movements, nor knowledge of with whom, or when, App users have been in contact with each other.

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

When 'Diagnosis Keys' are uploaded to AWS servers with your IP address, the IP address is stripped from the information at the earliest possible opportunity which renders the information anonymous.

Who processes your data

The DoH has overall responsibility for the app and has directed the Health and Social Care Board (HSCB) and Public Health Agency (PHA) to deliver services in relation to the app, as Data Processors on behalf of DoH. Therefore there are a number of data processors and sub-processors involved in the delivery of the app, who may process data in relation to the app.

Data processors

The following provides a list of data processors and sub processors involved in delivery of the app.

- NearForm are the app developers who will be providing technical support on the running of the app. Their services are delivered via HSCB GDPR compliant contracts.
- Big Motive Ltd are the design team who have worked with NearForm to design the user experience and content for the app.
- Gov.UK Notify provide the service to enable the sending of an SMS to your phone which contains the 'Authorisation Code' needed to enable your phone to release 'Diagnosis Keys'. Their services are delivered via HSCB GDPR compliant contracts. Amazon Web Services provide cloud storage and cloud services for the data uploaded from your phone. Their services are delivered via HSCB GDPR compliant contracts.
- The BSO provide certain services as a data processor on behalf of HSCB and PHA. The BSO host the Covid test registry for lab results. They operate the test registry, gathering the results of testing, positive test results to be notified via SMS text message, and be made available to PHA staff delivering manual contact tracing services, as well as associating results with electronic patient records to ensure appropriate access by clinical professionals supporting clinical care service delivery. They also provide backup support to the SMS function through arrangements with the HSCB. Their services are managed via appropriate agreements with PHA and HSCB.

Contracts and MoUs are in place to govern relationships with the above data processors and sub-processors which set out the obligations of each party and the data controller's obligations and rights with regard to the data that is being processed. All data processing takes place within the EEA area, and as such is subject to legislation in the form of the General Data Protection Regulation (GDPR).

Other recipients

The regional level data (outlined above) is extremely limited in scope. The DoH will make freely available the high level anonymised data, in order for members of the public to see the level of uptake, and the potential of the App to reduce the rate of spread of infection of COVID-19.

Anonymised diagnosis keys are shared with DoH IRL, via a federated server in ROI, in order to enable interoperability of the app cross border, to support users undertaking cross border travel. There is a MoU in place between DoH NI and DoH IRL in relation to this.

Data transferred outside the European Economic Area

No data will be transferred outside the EEA. All data processing will be subject to GDPR regulations and obligations.

How long your personal data is held for

No personal data is collected or stored, but we have outlined below how long certain data connected to the App are retained for.

Your IP Address:

Following upload of your IP address to AWS servers, it is deleted once the server network layer has routed the traffic to the application layer. User IP addresses are never transferred to the application layer.

'Identifier beacons' on your device:

This anonymous information is retained for 14 days.

Diagnosis keys in AWS registry (HSCB account set up on behalf of the DoH):

This anonymous information is retained for 14 days.

Diagnosis keys on your device:

This anonymous information is retained for as long as is necessary to perform a match check and is deleted thereafter.

Gov.UK Notify SMS Service

All SMS texts and phone numbers, processed on the server, are deleted once a SMS text message has been successfully transmitted. This 'server' is physically / electronically separated from the servers supporting the backend of the App. Different service teams will be employed to ensure that identifiable information (mobile phone numbers and test results) are kept separate from the App operational servers, preventing any individuals information being discoverable with the App.

The flow of data from the BSO test registry through the App backend to the Gov.UK Notify (SMS Platform) to send an SMS text will be managed by different groups to help reduce any risk of re identification.

- The BSO registry contains the mobile numbers of people who have tested positive.
- As the Temporary Exposure Key uploads hit the App backend in Amazon Web Services, it is important this backend data cannot be combined with mobile numbers.
- To help prevent this, the Amazon Web Services backend will never store or log the mobile number.
- The mobile number will exist in the BSO test registry and will exist in Gov.UK Notify as SMS messages are sent. (Being deleted after this action has been fulfilled).

To facilitate reconciliation for issues that may occur within the Amazon Web Services backend, a Job ID will be used to track the flow from BSO registry through Amazon Web Services. When BSO calls the Amazon Web Services REST API it will pass on a Job ID that will be used to uniquely identify the transaction with the Amazon Web Services flow.

This Job ID will be logged within Amazon Web Services so that in the case of any failure during processing, the record in the BSO registry that was not successfully processed can be identified.

In the case of a failure during the Amazon Web Services flow, an alert will be raised within Amazon Web Services and notified to the NearForm support team. The NearForm team will investigate alerts raised and will either address or correct, if the issue is within Amazon Web Services.

If the issue is outside of Amazon Web Services, when appropriate, NearForm will escalate the issue to the BSO support team.

BSO will be required to reconcile the Job ID from registry data to the SMS text records on the Gov.UK Notify platform.

The PHA manual Contact Tracing service will also be telephoning all positive test users, so can be scripted to verify that the recipient has received a SMS; the call handler will also have the capability of sending an SMS from the Manual Contact Tracing system.

DoH / HSCB / PHA- Regional Summary Level Information

The DoH / HSCB / PHA will retain regional summary level information, relating to the number of App users / ratio of exposure notifications to positive cases indefinitely, to support evaluation of the App's effectiveness in pursuance of CE accreditation. This process will be conducted in line with requirements outlined by the MHRA, the regulator.

This regional level data will be retained for purposes of research and future pandemic response planning. This does not involve individual data. Though interim approval has been granted, in order to obtain formal MHRA Regulatory approval, and CE certification, will involve collation of data in evidence of the efficacy of the App. In line with GMGR Disposal Schedule J - Clinical Trials of Investigational Medicinal Products (CTIMPs) – this high level summary data will be retained *'for an appropriate period, to allow further analysis by the original or other research teams subject to consent, and to support monitoring by regulatory and other authorities'*. https://www.health-ni.gov.uk/articles/disposal-schedule-section-j

On occasion of the pandemic being declared as having ended, the App will be stood down. Users will be instructed to delete it from their phone. Any anonymised data present, at that time, in the AWS servers (on behalf of the DoH to support the App function) will be deleted.

Data Subject rights

Users have rights under GDPR when their personal data are processed by data controllers. The following considerations should be noted. IP addresses are not retained on the app backend, but for transient network routing and network security purposes. Diagnosis keys are not capable of being associated with a person as they are non-identifying by design.

- **Right to information** – a Data Protection Privacy Notice (Notice) is provided via the app itself on those pages which request information and also in the app Settings. The Privacy Notice will also be published on the DoH website. The Notice contains information as prescribed under Article 13 and 14 of the GDPR.

- **Right to rectification** – since no personal data is collected or retained by DoH, it would not be possible for DoH to comply with a request for rectification.

- **Right of access** – since no personal data is collected or retained by DoH, it would not be possible for DoH to comply with a request for access.

- **Right to erasure** – the user can select the Leave function, delete the app at any time, and delete ENS data via device settings – erasing all data processed on the phone. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for erasure.

- **Right to restriction** – the user can revoke their ENS permission, revoke their exposure notification permission and decide not to upload keys. Ultimately the user can decide to Leave and/or delete the App from their device. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for restriction.

- **Right to portability** – it is not possible for users to port their keys, for example, from one device to another device as the user does not have access to such keys on their device (save to delete them) and as regards those uploaded to the DoH, the DoH cannot identify which keys belong to which user. Since no personal data is collected or retained by DoH it would not be possible for DoH to comply with a request for portability.

- **Right to object** – the user can use the Leave function to delete the information from the app; the user can delete the app from their device and the user can delete ENS data via device settings.

- **Right not to be subject to solely automated decision-making including profiling** – if the ENS detects a match between a Rolling Proximity Identifier on the App and a Diagnosis Key downloaded from DoH Diagnosis Key Registry, a decision is made that a close contact has taken place. This decision is based solely on the automated processing of identifiers and keys and does significantly affect users. However, this processing is based on the explicit informed consent of the user, during the on-boarding process. The automated decision-making is an essential feature of the proximity app solution provided, and is core to nits function in delivering the public health objective of infection control. If App users wish to speak to someone in relation to an 'Exposure Notification' that they have received via the App, they can call '**0300 200 7896**' and select the option to speak to someone about the notification at the following times: Monday-Friday (excluding bank holidays) between the hours of 8:30am – 5:30 pm. Someone will answer the call and explain the 'Exposure Notification'. They will have no way of knowing with whom, where or when a 'high risk' contact took place, but they will try to explain the process to App users and its purpose. **App users can express their point of view and contest the decision.** These steps should enable the App user to make an informed decision as to whether to self-isolate to prevent spreading the infection to others. Ultimately if they are still not satisfied or need clinical advice they will be advised to seek clinical assessment by their GP or GP OOH.

Changes to this Data Protection Information Notice

This Data Protection Information Notice may change from time to time and you will receive notification of this update in the app.

How to complain if you are not happy with how we process your personal information

If you are unhappy with any aspect of this privacy notice, or how your personal information is being processed, please contact the Department's Data Protection Officer at the address above.

If you are still not happy, you have the right to lodge a complaint with the Information Commissioner's Office (ICO):

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 0303 123 1113
Email: casework@ico.org.uk

Website: Information Commissioner's Office

Version 6.0. 31st July 2020

Appendix K – Terms and Conditions

Terms and conditions

Please read these terms of use carefully. By downloading this COVID-19 NI Contact Tracing App you agree to these terms.

Introduction

These are the terms of use for the COVID-19 NI Proximity App (also referred to as StopCOVID NI) which is being made available by the Department of Health (DoH) in Northern Ireland (under powers available through the 'Health and Social Care (Reform) Act (Northern Ireland) 2009'). The App has been designed to assist in stopping the spread of COVID-19 in Northern Ireland, by anonymously contacting people who have been in close contact with someone who has tested positive for COVID-19. The App has been developed on behalf of the DoH for the benefit of citizens in Northern Ireland.

The phones of those who are using the App emit anonymised coded 'keys', 'Identifier Beacons', which change every 15 minutes. These 'keys' are stored on the user's phone for 14 days before being discarded. When close to each other, App users' phones exchange these anonymous 'keys', and if they are in close proximity with another user for a significant period of time, both will store the anonymous 'key' of the other phone for 14 days.

'Authorisation Codes' are anonymous random six digit alphanumeric codes generated to verify that a positive test has been received by the App user, allowing 'exposure notifications' to be sent via the App, when the user enters a valid 'authorisation code.' On entering the code, the user is asked to release the anonymous keys their phone has transmitted over the previous 14 days: these are then known as 'diagnosis keys'. These are then released to the secure registry supporting users of the App, to be shared with other App users.

'Diagnosis keys' are anonymised identifiers generated on entry of an 'authorisation code' on the App, and stored in a secure registry, maintained in a Health & Social Care Board secure cloud services account (on behalf of the DoH) on Amazon Web Services (based in London). Every App user's phone regularly checks for 'diagnosis keys' and where these match a significant contact episode's anonymous 'key' stored on their phone, over the previous 14 days, an 'exposure notification' is enabled. The notification is generated on the App user's phone, not in the secure registry.

Where 'Exposure Notification' is mentioned, this refers to an anonymous notification, received via the App, that you have been in contact with an unnamed individual who has tested positive for COVID-19, and that contact was recent enough, and for sufficient time, at a close enough distance to mean that you may have been infected.

Please read these terms of use in conjunction with the Privacy Information Notice for the App, available to view below.

References to "DoH", "we" and "us" in these terms of use are to the Department of Health NI which is the owner and licensor of the StopCOVID NI Contact Tracing App. References to "the user" and "you" refer to the person who has downloaded the App onto their device for their own personal use and who uses the service.

Version 6.0. 31st July 2020

Department of Health
An Roinn Sláinte
Männystrie O Poustie
www.health-ni.gov.uk

What the StopCOVID NI Contact Tracing App does

The StopCOVID NI Contact Tracing App only provides one function, namely 'exposure notification'. It is a clearly declared position that no further functions will be added to this App, and that use of GPS location functionality will **NOT** be added at any time by the DoH.

Exposure Notification

The App records if users are in close contact with another App user (see above). If an App user tests positive for COVID-19 the App will notify any App users that have been closer than two metres for more than fifteen minutes (this is in line with current public health policy, and can be changed depending on advised best practice), in the previous 14 days. The App uses capabilities of mobile operating systems. Apple and Google have developed a method that allows specific government-only COVID-19 Apps to make use of Bluetooth technology on phones that would otherwise not be available. As the App will need to use the most current version of the phone's operating system, users may be asked to upgrade the first time they use it. None of the information in this App is ever shared with Apple or Google. The App cannot be used on older phones, on which it is not possible to upgrade the operating system. It is not available on phones which use a different operating system, other than the Android or iOS systems deployed by Google / Apple.

First time use

The first time anyone uses the App they are prompted to allow the App to collect and share the anonymous data transmitted by nearby devices that also have the App installed.

Metrics Data

Metric data does not identify you and is used to create aggregate views of how the App is being used and the impact it is having on the virus. Here is a list of the App metrics which, are collected from your App. The collection of these metrics is essential in order to prove efficacy and gain CE accreditation.

1. The total number of App users
2. The total number of instances where 'diagnosis keys' have been uploaded
3. The total number of 'exposure notifications' triggered

The DoH will not know any of these instances related to any individual app user, simply total numbers (for the region) of 'authorisation codes' and 'exposure notifications' in any given time period.

If you are notified that you have been in close contact with someone who has tested positive, you will be advised to self-isolate for 14 days. If you have symptoms you will be directed to check your symptoms at https://covid-19.hscni.net/ (where you can download the 'COVIDcare NI' symptom checker App if you do not already have it) and book a test.

Use of the StopCOVID NI Contact Tracing App.

The StopCOVID NI Contact Tracing App is free to download and use to anyone who is resident in Northern Ireland. The Service is intended only for people resident in Northern Ireland and the Service may not be otherwise used.

Version 6.0. 31st July 2020

Users downloading the App who are not resident in Northern Ireland will not be able to receive authorisation codes, in relation to a positive test for COVID-19, as the app is linked to the NI test registry (which only receives results in relation to people resident in Northern Ireland). On downloading and activating the App, users are asked to confirm that they are resident in Northern Ireland and, if not, are discouraged from using the App with an explanation that it will not work for them. They are encouraged to use an App intended to cover their own area.

It is intended that the StopCOVID NI Contact Tracing App will be able to be used by those resident in Northern Ireland visiting anywhere in the Republic of Ireland; and it is intended that those using the App launched in the Republic of Ireland may use that App when visiting Northern Ireland. This will be achieved by delivering 'interoperability'. 'Interoperability' is achieved by the secure sharing of anonymous 'diagnosis keys' on a secure shared 'federated server' hosted on the Dublin AWS account of the DoH IRL. The server is only accessible to the apps of app users, and is not otherwise accessible. The server only contains non-identifiable data, 'diagnosis keys stripped of any indefinable information, and as such falls out with the scope of GDPR. This is governed by a bilateral agreement between the Departments of Health in both countries, a MOU. It is not accessible by any other means other than the Apps of the two countries. It is intended that as other countries release similar Apps, more agreements will be reached to share anonymous 'diagnosis keys', enabling users of the StopCOVID NI app to use the app visiting other countries. These 'keys' cannot be used to identify any individual, and are totally anonymous. The ability for App users who travel to be able to receive notifications, and enable others to receive notifications if they test positive is important to help stop spread of COVID as people start to travel again.

Use of the App requires an Android or iPhone mobile telephone device which supports Android 6.0 or higher (in the case of Android phones) or iOS 13.5 or later (in the case of iPhones). In addition, in order to operate correctly, the App also requires Bluetooth functionally turned on and the COVID Exposure Notification service enabled.

If you consent to the Exposure Notification service provided by the App and want to receive those services, you will need to enable Bluetooth and location services and you will need to permit push notifications from the App. The App will prompt you about enabling these services and providing permissions if and when you give your consent to receive the service from the App. The App does not use GPS location services, or Google location services to track your movements. The App simply uses the strength of the Bluetooth signal of phones, with the App activated, to measure the proximity of those phones, and the length of time spent at a given proximity.

More about the DoH and the licence to use the App

We license you to use:

The Covid-19 Contact Tracing mobile application software and the data supplied with the software (the StopCOVID NI Contact Tracing App) and any authorised updates or supplements to it;

The related online or electronic documentation related to the App (Documentation), and The Services you connect to via the App and the content we provide to you through it, as outlined above, subject to and as permitted in these terms.

The above licence is a personal, non-exclusive, non-transferable, revocable, limited licence to use the StopCOVID NI Contact Tracing App and the Documentation, and through the App to use the Services, for your own personal use. All other licence rights not expressly permitted are fully reserved to us.

If you want to report back to us about your experience of using the StopCOVID NI Contact Tracing App, or want to report any problems with the use of the App or the Services, please contact us by calling '0300 200 7896' and selecting the option to speak to someone to log a request, at the following times; Monday-Friday (excluding bank

holidays) between the hours of 8:30am – 5:30 pm. You will also find more information at https://covid-19.hscni.net/

Your Privacy

We only use any data we collect through your use of the App and the Services in the ways set out in our Privacy Information Notice. The Privacy Information Notice confirms the terms upon which your data is collected and used in respect of your use of the App and the Services.

App Store's terms also apply

When you download the App, or when you access or use the App or the Services, you may also be subject to the terms of use and policies of the relevant App Store (Google Play Store or Apple Store) from which you download the App. Please review these terms of use and policies very carefully. Your access to, and use of, the Services will be governed by these (the DoH's) terms of use, unless the terms of use and policies of the relevant App Store say otherwise.

How you may use the App, including how many devices you may use it on

In return for your agreeing to comply with these terms you may:

- download a copy of the App onto one mobile device and view, use and display the App and the Services on this device for your personal purposes only,
- use any Documentation to support your permitted use of the App and the Services,
- provided you comply with the licence restrictions above, make one copy of the App and the Documentation for back-up purposes, and
- receive and use any free supplementary software code or update of the App incorporating "patches" and corrections of errors as we may provide to you.

You must be 18 to accept these terms and to download and use the App

You must be at least 18 years of age in order to accept these terms and to download and use the App.

The right to use the App and Services is personal and you may not transfer the App to someone else

We are giving you personally the right to use the App and the Services as set out above. The use of the App by multiple individuals from the same device undermines the accuracy and efficacy or the App's contact tracing function (if enabled). If you permit someone else to access your device and to use the App or Services, then you do so at your own risk, and you are responsible for that person's use and you must ensure that the person knows about and complies with these terms. You must also not use any other person's StopCOVID NI Contact Tracing App.

You may not otherwise transfer the App or the Services to someone else, whether for money, for anything else or for free. If you sell any device on which the App is installed, you must first remove the App from the device.

Version 6.0. 31st July 2020

Changes to these terms

We may need to change these terms to reflect changes in law or best practice or to deal with additional features which we introduce.

We will give you at least 7 days' notice of any change by sending you an in-App notification and providing you with details of the change, on this publication, and notifying you of a change when you next start the App.

Changes driven

Northern Ireland Public health policy may not be subject to the 7 days' notice, as the timing of implementation may not allow it. We will publicly notify changes in the app and on https://covid-19.hscni.net/stop-covid-ni-mobile-app in advance.

If you do not accept the notified changes, we will advise you what specifically this will mean at the date of the notification. It may mean that you will not be permitted to continue to use the App and the Services. This will be your informed choice.

Updates to the App and changes to the Services

From time to time we may automatically update the App and change the Service settings to improve performance, enhance functionality, reflect changes to the operating system or address security issues. Alternatively, we may ask you to update the App for these reasons. If you choose not to install such updates or if you opt out of automatic updates you may not be able to continue using the App and the Service, and you may compromise the security of your data or device.

If someone else owns the phone or device you are using

If you download or stream the App onto any phone or other device not owned by you, you must have the owner's permission to do so. You will be responsible for complying with these terms, whether or not you own the phone or other device.

We are not responsible for other websites you link to

The App or any Service may contain links to other independent websites which are not provided by us, such as websites for purposes of booking a test. Such independent sites are not under our control, and we are not responsible for and have not checked and approved their content or their privacy policies (if any). You will need to make your own independent judgement about whether to use any such independent sites.

Licence restrictions

You agree that you will:

- except in the course of permitted sharing, see information on how you may use the app above, not rent, lease, sub-license, loan, provide, or otherwise make available, the App or the Service in any form, in whole or in part to any person without prior written consent from us, nor will you infringe our rights (including our intellectual property rights) in relation to your use of the App or Services;

- not copy the App, Documentation or Services, except as part of the normal use of the App or where it is necessary for the purpose of back-up or operational security;
- not translate, merge, adapt, vary, alter or modify, the whole or any part of the App, Documentation or Services nor permit the App or the Services or any part of them to be combined with, or become incorporated in, any other programs, except as necessary to use the App and the Services on devices as permitted in these terms;
- not disassemble, de-compile, reverse engineer or create derivative works based on the whole or any part of the App or the Services nor attempt to do any such things, except to the extent that (by virtue of 'The Copyright (Computer Programs) Regulations 1992') such actions cannot be prohibited because they are necessary to decompile the App to obtain the information necessary to create an independent program that can be operated with the App or with another program (Permitted Objective), and
- provided that the information obtained by you during such activities is not disclosed or communicated without our prior written consent to any third party to whom it is not necessary to disclose or communicate it in order to achieve the Permitted Objective, is not used to create any software that is substantially similar in its expression to the App, kept secure; and is used only for the Permitted Objective,
- comply with all applicable technology control or export laws and regulations that apply to the technology used or supported by the App or any Services.

You must:

- ensure that all information that you provide to us via the App is accurate, complete, honest and not misleading, to the best of your knowledge, information and belief;
- comply with all applicable laws and regulations in using the App and the Services;
- not use the App or any Service in any unlawful manner, for any unlawful purpose, or in any manner inconsistent with these terms, or act fraudulently or maliciously, for example, by hacking into or inserting malicious code, such as viruses, or harmful data, into the App, any Service or any operating system;
- not infringe our intellectual property rights or those of any third party in relation to your use of the App or any Service, including by the submission of any material (to the extent that such use is not licensed by these terms);
- not transmit any material that is defamatory, offensive or otherwise objectionable in relation to your use of the App or any Service;
- not use the App or any Service in a way that could damage, disable, overburden, impair or compromise our systems or security or interfere with other users; and
- not collect or harvest any information or data from any Service or our systems or attempt to decipher any transmissions to or from the servers running any Service.

Intellectual property rights

All intellectual property rights in the App, the Documentation and the Services throughout the world belong to us and the rights in the App and the Services are licensed (not sold) to you. You have no intellectual property rights in, or to, the App, the Documentation or the Services other than the right to use them in accordance with these terms.

Our responsibility to you

No warranty. While we take every care to ensure the correctness of the information, content and communications published in the app, we make no representation, warranty or guarantee as to the correctness, accuracy, completeness, currency or reliability thereof. We assume no responsibility and make no warranty that the functions and use of the App will be permanently and continuously available and free of errors or faults, that errors will be rectified, or that the App will be free of viruses or other harmful elements.

Exclusion of liability. To the extent permitted by law, any claims for liability against us due to material or immaterial damage, including indirect or consequential damage, arising for example from access to, use or non-use of the App and the associated information, content and communications, from misuse of the connection or technical faults or any other loss or damage whether arising under tort (including negligence), breach of contract, breach of statutory duty or otherwise, are hereby excluded.

We do not exclude or limit in any way our liability to you where it would be unlawful to do so. This includes liability for death or personal injury caused by our negligence or the negligence of our employees, agents or subcontractors or for fraud or fraudulent misrepresentation, or in respect of any of your legal rights as a consumer (to the extent that these cannot be excluded).

Limitations to the App and the Services. While the App provides notification to those who may have been exposed to a confirmed positive case, providing advice to self-isolate, the App provides no additional functions. All those in Northern Ireland with a positive test result for COVID-19 would be expected to receive a phone call from a clinical professional employed on the Test Trace and Protect programme. This public health service, provided in Northern Ireland, is separate from the App and works in parallel. The App works in an anonymous and automated way, in parallel to the manual Test Trace and Protect contact tracing process. Information from the app is not shared with those working in the manual service.

Automated processing. The generation of exposure notices on the app is an automated process, not involving a human. The automated process is carried out by use of anonymous identification keys, and measurement of Bluetooth signals to calculate that App users' phones have been close enough for long enough to constitute a significant contact, sufficient to put you at risk of having been infected. It is necessary for the app to do this in an automated way, in order to protect your identity and the identity of other app users. If you need to discuss this with an individual, you can call '**0300 200 7896'** Monday-Friday (excluding bank holidays) between the hours of 8:30am – 5:30 pm. **App users can express their point of view and contest the decision.**

Withdrawal of or changes to the App or Services. The App and Services are intended to be made available for a limited period only while the Covid-19 crisis is ongoing. Without prejudice to this, we expressly reserve the right, at any time, without prior notice, to withdraw the App and Services. We also expressly reserve the right, at any time, and without prior notice, to make changes and/or improvements to the App and Services.

Please back-up content and data used with the App. We recommend that you back up any content and data used in connection with the App, to protect yourself in case of problems with the App or the Service.

Check that the App and the Services are suitable for you. The App and the Services have not been developed to meet your individual requirements. Please check that the facilities and functions of the App and the Services (as described on the App Store site and in the Documentation) meet your requirements.

We are not responsible for events outside our control. If our provision of the Services or support for the App or the Services is delayed by an event outside our control then we will contact you as soon as possible to let you

know and we will take steps to minimise the effect of the delay. We will not be liable for delays caused by the event, but if there is a risk of substantial delay you may contact us to end your use of the App at any time.

You can end your use of the App and what happens if you do

You can stop using the App at any time, and you can delete it at any time from your device.

If you delete the App, you will not be able to access the Services, and all rights granted to you by these terms will cease. We will not be holding any personal data in relation to you, since we will not be collecting any; however any data held on your phone can be removed as indicated in the App instructions. Details are provided in relation to data processed by the App in the Privacy Information Notice.

We may end your rights to use the App and the Services if you break these terms

We may end your rights to use the App and Services at any time by contacting you if you have broken these terms in a serious way. If what you have done can be remedied we will give you a reasonable opportunity to do so.

If we end your rights to use the App and Services:

- You must stop all activities authorised by these terms, including your use of the App and any Services.
- You must delete or remove the App from your device(s) and immediately destroy all copies of the App which you have and confirm to us that you have done this.
- We may end support and linkage to the App, form the App backend, rendering the App redundant.

We may transfer our rights and obligations to someone else

We may transfer our rights and obligations under these terms to another organisation. We will always tell you in writing if this happens and we will ensure that the transfer will not affect your rights under the terms of the licence.

You need our consent to transfer your rights to someone else

You may only transfer your rights or your obligations under these terms to another person if we agree in writing.

No rights for third parties

In respect of any individual not resident in Northern Ireland downloading and using the App: it is clearly our stated intent, that this app should **not be used by individuals who are not resident in Northern Ireland**. In order to avail of the App's functionality in terms of exposure notification, it is essential that users are resident in Norther Ireland, in order for us to be able to deliver authorisation codes in relation to their test results. During the on-boarding process, App users are given clear instruction not to use the App if they are not resident in Northern Ireland, and that the App functionality will not be available to them. As a result, we can accept no liability for anyone ignoring the instruction and using the App improperly.

If a court finds part of these terms illegal, the rest will continue in force

Each of the paragraphs of these terms operates separately. If any court or relevant authority decides that any of them are unlawful, the remaining paragraphs will remain in full force and effect.

Even if we delay in enforcing these terms, we can still enforce them later

Even if we delay in enforcing these terms, we can still enforce them later. If we do not insist immediately that you do anything you are required to do under these terms, or if we delay in taking steps against you in respect of your breaching these terms, that will not mean that you do not have to do those things and it will not prevent us taking steps against you at a later date.

Terms survive

Any of these terms of use that are intended to come into or continue in force on or after termination or expiry of these terms (which includes for the avoidance of doubt the provisions dealing with *Our responsibility to you*) will remain in full force and effect following termination or expiry. Termination or expiry of these terms of use shall not affect any rights, remedies, obligations or liabilities of you or us that have accrued up to the date of termination or expiry, including the right to claim damages in respect of any breach of the terms of use which existed at or before the date of termination or expiry.

Which laws apply to these terms and where you can bring legal proceedings

These terms are governed by the law of Northern Ireland and you can bring legal proceedings in respect of these terms (or anything to do with the App or the Services) in the courts in Northern Ireland only.

Version 6.0. 31st July 2020