Department of Health & Social Care

The NHS COVID-19 app (Late April 2021 release):

Data Protection Impact Assessment

Published 28 April 2021

Published to GOV.UK in pdf format only.

NHS Test and Trace, NHS COVID-19 app

www.gov.uk/dhsc

Contents

The app and app user in context

The Department of Health and Social Care (DHSC) is the data controller for several services provided to members of the public (data subjects). DHSC is responsible for taking steps to protect the privacy of individuals, to reduce their identifiability and to ensure that processing is proportionate, and that safeguards are in place. For example, as service users pass through systems, this means ensuring that only the minimum amount of data necessary is shared between services and data sets are held separately.

In the context of a pandemic (a public health emergency), data sharing between services is necessary to support the management of communicable diseases and for the protection of the public. This includes monitoring the effectiveness of services and their impacts on different communities.

This DPIA is updated to reflect new functionality introduced to the NHS COVID-19 App (the “app”) which supports the NHS Test, Trace and Protection service in Wales and the NHS Test and Trace service in England. You can find a summary of these changes in the section Update to the Data Protection Impact Assessment (DPIA) for the NHS COVID-19 App.

This DPIA is updated to reflect new functionality introduced to the NHS COVID-19 App (the “app”) which supports the NHS Test, Trace and Protection service in Wales and the NHS Test and Trace service in England.

More information our work with health services in Gibraltar, Jersey, Northern Ireland and Scotland can be found in the section working together.

The app user (the app data ecosystem)

The use of data collected from app users is subject to the controls and oversight detailed in this DPIA and associated privacy notice.

The law requires a clear commitment from the Department of Health and Social Care to maintain the user’s privacy and protect their identity from other app users and the government. The user journey and data flows are shown in diagrams throughout this document. More detail is provided within the appendices and annexes of this document.

Any change to the data requested will be reviewed, will be lawful, and will be available as an additional choice by the user. Please note that any future changes beyond the scope of the current version of the app will be reflected and updated in this data protection impact assessment (DPIA).

Data generated and collected by the app is held in 3 environments. Systems are in place which support the secure and appropriate flow of data between these environments:

- app users' phone – the NHS COVID-19 App and the majority of data collected by the Apple/Google API will be always (and only) held on the app user's phone. This is considered a user-held record. For most functionality, data is presented to the user's phone and is checked against the data held on the phone (for example, visited venue QR codes that could be considered at risk or other users that should be considered at risk)

- product environment – certain data items are collected from user devices (via an API) to allow core features of the app to work and be managed effectively. This data collection includes details of the phone type and operating system and the user provided area information (postcode district and local authority). These items are described in the data dictionary set out in appendix 1 of this document. Within the product environment service performance dashboards are provided to support the oversight and management of the app and associated services. Data and access is kept within the control of the DHSC.

- analytical environment – derived data from the app will flow to the analytical environment to support learning about the app and COVID-19. All data held in the analytical environment is subject to strict de-identification controls to ensure datasets are de-identified and aggregated.

Virology testing

App users who enter symptoms and are recommended to seek an approved COVID-19 virology test can generate a reference code ("test code") unique to themselves and to the particular occasion on which they seek a test.

The test code gives the user access to the virology testing website where they can book a test. The functionality of the app will ensure that the test code is transferred to the website. In order for a test to be booked and the results sent to the correct individual, the website requests additional data from the user.

The test result and code are used to feed results back to the app. Where the user enters the result via a code or by the app systems, it collects the type of test, the test result and the relevant dates.

This will:

- update the user's COVID-19 status

- add, where appropriate, the relevant code to the list of “at risk” individuals presented to app users’ phones (triggering an update in the status of app users if their “Exposure Log” includes the protected identification code of the individual)

- where appropriate, in line with the current testing policy, recommend the app user seeks a confirmatory test;

- note the relevant type of test in the app and the requirement for a confirmatory test, in the operational, analytical data sets and exposure windows as required.

As noted in this DPIA, the app allows the user to add a test result into the app without a test code generated from within the app. These includes the type of test which includes test results entered by the user. App users who have tested positive for COVDI-19 will be prompted to enter an onset of symptoms date when one is not available. This allows the app to recommend to the user when their isolation should start and end.

The app aligns with the COVID-19 testing policy in England and Wales. Where confirmatory testing is recommended, the app will recommend this to the user. For details of the latest COVID-19 testing policy in England and in Wales see the following links:

- COVID-19: guidance for households with possible coronavirus infection - GOV.UK (www.gov.uk)

- https://www.gov.uk/getting-tested-for-coronavirus

- https://www.gov.uk/guidance/coronavirus-covid-19-getting-tested

- Testing for coronavirus | Sub-topic | GOV.WALES

Venue (QR) alerting system

Venue alert data is presented as a list of “at risk” QR codes (protected to obscure the location) sent out by the system to the app. This data triggers the alert functionality within the app.

Using QR codes to check in at venues is a more robust privacy preserving mechanism for the user than manually signing-in with a pen and paper.

This function does not relate directly to the data processed within the app.

To enable users to put this function in context, we set out below how the QR check in function works for venues, and how the process functions end to end below.

Creating a QR poster

Venues are able to create a NHS Test and Trace QR code by using the GOV service available. The QR generator resides in a sub AWS account of the NHSX domain, distinct from the app.

They will need to provide the following details:

- an email address – used to send a 6-digit verification code, required to continue the QR generation process.
- name – used to personalise the email sent with the link to the poster.
- type of venue – denotes the type of venue which his included as QR codes are not mandatory in all venues.
- venue name – this is displayed on the poster.
- address – displayed on the poster.
- contact email address and phone number for responsible person – used in case of need to contact venue.

An official T&T QR poster will be generated and emailed to the recipient, to be displayed at their venue.

Checking in

An app user is able to check in to a venue by scanning the QR code using the NHS COVID-19 App. When they check in, the venue name, date and time is shown to the user so they can verify the details (and cancel if necessary). The venue name, unique poster ID, date and time are stored on their device for up to 21 days, and this list is visible to the user. The user is able to delete any entries from this list.

If a user scans a third-party QR instead of the official COVID-19 the app will immediately alert the user, advising them the QR code is not recognised and it could be that they didn't scan an official NHS QR code (or the code is damaged).

Identification of outbreak at a venue

Local Health Protection Teams (HPT) are responsible for local outbreak management. PHE consultants within the HPTs will investigate clusters to determine if there is an outbreak. They may receive information from a venue itself (reporting that staff/customers have tested positive), or through the Contact Tracing and Advice Service (CTAS)

information which captures details provided voluntarily by persons who have tested positive, via a contact agent or an online webform. They use existing processes and log details in the HP Zone case management tool. This is outside of the scope of this DPIA.

Triggering the notification in the app

Secure two-factor authentication is used to access the Venue Risk Notification tool. This resides in the sub-AWS account in the NHSX domain, and provides a list of venues which have created a QR poster. In this system it is possible to:

- search by Postcode or Poster ID and select a venue.
- once selected, a date/time from/to will be selected, depending on the assessment they have carried out
- When the venue is flagged in the Venue Risk Notification Tool:
- an API call is made into the app backend system.
- the app system sends the list of QR IDs into the app for all app users.
- the app will match against the user's venue history, and if a match is identified it will trigger a notification to that user. There are two notification types depending on the number of cases:
    - Warn and Inform: "You recently visited a venue on the same day as others who have since tested positive for coronavirus (COVID-19)."
    - Warn and Book a Test: "You recently visited a venue where there's been an outbreak of coronavirus (COVID-19)."
- the notification does not display the venue name

Contact tracing (national)

No data from app users is passed to any of the national contract tracing systems in use. App users can choose to use the information held only on their phone to support the contact tracing process when interacting with the service. Data collection and use is governed by the DPIA and privacy notice alongside processes used by that service. No data is shared from the app.

An option being considered is to allow app users the choice to send data held on their phone to contact tracers. This is not currently available as a feature, but if adopted would allow the user to share details of the venues they have visited.

This option is subject to a change control review - including a review of the legality, proportionality and impacts upon privacy and identifiability.

Contact tracing (local)

The same conditions apply to any local contact tracing by local public health teams. The app user may use the data held only on their phone to assist themselves and the contact tracer, if they choose to.

Supporting the wider Public Health response to NHS COVID-19

The Department of Health and Social Care has tasked NHS Test and Trace with leading the Test, Trace and Contain public health strategy and interventions in response to coronavirus (COVID-19). The NHS COVID-19 app is intended to influence and inform the behaviours of app users and the public to reduce the transmission of COVID-19. App users continue to contribute to the public health response to COVID-19 through their use of their app and the data using the app's functions generates.

The data collected to enable the functions and impacts of the app can be further analysed and used alongside other data to target public health actions and inform public health actions. This requires no additional data to be collected or processed by the app and can be done whilst maintaining the privacy and identity of app users. This aggregate data referred to as aggregate derived data in this document and is used by the wider Test and Trace service and Local Public Health functions to inform their public health interventions.

For more information see the section Flows of Aggregate Data Derived from the app.

Update to the data protection impact assessment (DPIA) for the NHS COVID-19 app (Late April release)

This DPIA was updated with the changes to the late April release for the NHS COVID-19 app. This change incorporates the updates from the releases on the following dates:

- 23 March 2021;
- 27 April 2021;

Updated Functionality and Support for App Users

- Warn and Book message for app users who have attended a venue that may pose a potential risk of COVID-19 infection, advising them to book a COVID-19 test;
- App users who test positive for COVID-19 are asked to share their Diagnosis Keys, which enables the Exposure Notification process. In addition, to the initial request app users now have a second opportunity to share their Diagnosis Keys;
- In alignment with broader testing and isolation policy, app users who have received Exposure Notifications but are not experiencing symptoms can now request a test;
- Improvement to the working of the app across platforms to ensure a more consistent experience for app users.

Points of Clarification (Data Flows)

The DPIA was updated to provide a brief overview of data that the app contributes to the wider Public Health response to COVID-19.

This aggregate data is derived from the data (“aggregate derived data”) collected by the app and which is strictly necessary for its functions and their validation.

This data is provided in aggregate form and further disassociated with specific app users. Details can be found in section Flows of data derived from the NHS COVID-19 app.

These data flows are:

- Aggregate derived data to the Test and Trace Data Analytical Platform(s);
- Public Dashboards.

The app does **not**:

- Provide user row level data (i.e. details of specific app users);
- Constitute Personal Data and is prevented from being processed being processed in a way that would increase the risk that it could be considered personal data;
- Does not track app users;

Ongoing Use of this data is bound by:

- Commitments made in this DPIA
- The Secretary of State's Ethical Framework for the NHS COVID-19 app;
- Ongoing oversight by the Department of Health and Social Care.

The March update to the DPIA included details about the changes to the Isolation Support Payments.

Changes to information held on the App: Adding Venue Postcode

When app users scan in venues, the code will now include the postcode for the venue.

- Following feedback from app users, Local Health Protection Teams and the Contact Tracing Advisory service there are ongoing issues with specifying the precise venue;
- Including the postcode of the venue allows the app users to identify the specific venue when needed;
- See the Privacy Notice for the Venue Check-In service for more information for venues and those using NHS QR Check-In codes;
- The postcode is included in the QR code that the user scans and populates the data in app without reference to any centralised system.

Updates to the DPIA

The data dictionary, see Appendix 1, and risk register, see Section 7 Risk Register, were updated in line with these changes.

Next steps for the app and the DPIA

The DPIA for the app continues to be subject to routine review, as significant changes are identified the DPIA is updated. A new version of the DPIA will be published when major updates to the app are released.

Apple and Google

The NHS COVID-19 App is available through the Apple App Store and the Google Play Store. Apple and Google provide the app independently of the NHS and Department of Health and Social Care.

For app user's using older versions of the app, Apple and Google are responsible for exposure notification messages sent to users which are outside of the remit and control of the NHS and DHSC. In response to this notification, the NHS COVID-19 app provides a clarification message to explain the level of risk and actions recommended as a consequence.

We recommend routinely updating the app to ensure you have the latest functionality and best performance of the NHS COVID-19 app.

For more information about Apple and Google's digital contact tracing technology see their websites.

The NHS Test and Trace app: data protection impact assessment

Introduction

The NHS COVID-19 app (“app”) is a mobile phone application that is part of the NHS Test and Trace Service, which is designed to break the chains of transmission of COVID-19. By using the app, users will help to protect themselves and those around them – their friends, family, colleagues and local communities, and enable society to return to a more normal way of life. The app is a medical device providing maximum freedom at minimum risk.

The objectives of the app are to:

- create an enduring new medical technology to manage public health
- promote behaviour change by helping people manage their risk exposure
- identify and inform people to help communities manage public health emergencies
- reduce disease transmission by giving users easy access to health services
- support and inform users during isolation

The behaviour sought by the app from users is to:

- download the app and use it daily
- keep the app ‘on’ and carry their phone at all times
- follow instructions issued by the app
- ‘pause’ the app when appropriate
- enter symptoms and take a test quickly when told to
- self-isolate (as we expect of everyone) if a user tests positive for COVID-19

Any “pause” of contact tracing needs to be resumed manually by the user. This is not an automated function.

The NHS COVID-19 App has 3 core roles:

- precision: to measure distance and time between app users accurately

- reach: to remember which other app users an app user has been near
- speed: to initiate self-isolation quickly through contact detection of positive cases

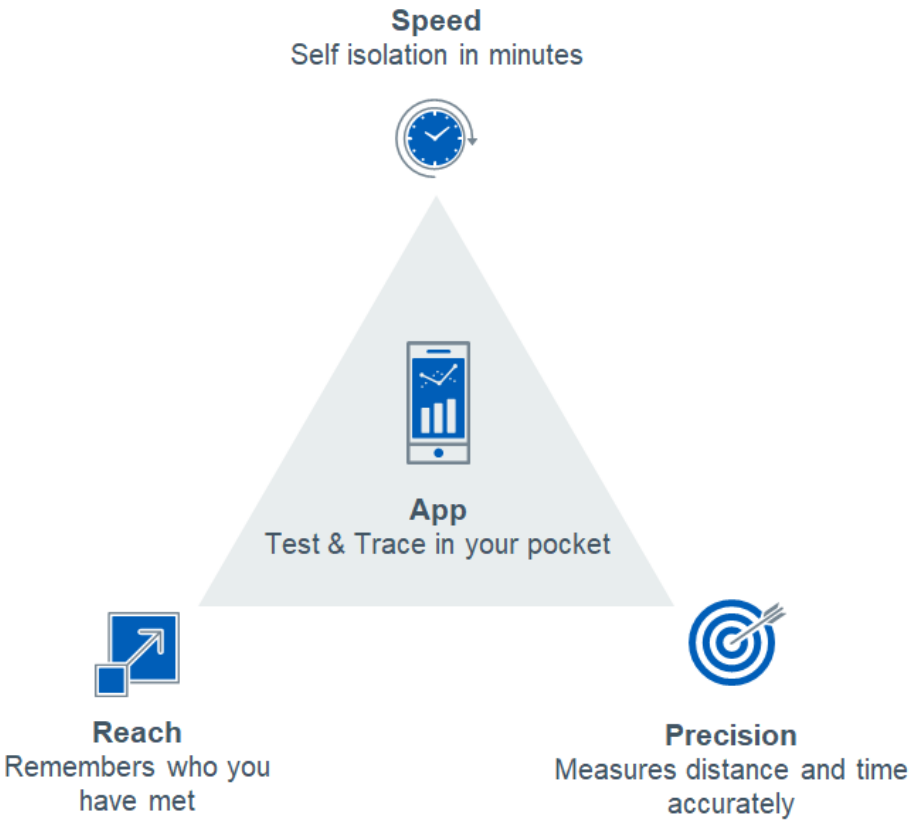


Figure 1: The 3 core roles

The data controller

On behalf of the Secretary of State, the Department of Health and Social Care (DHSC) will act as controller for the processing of personal data that supports the functioning of the app. This is overseen by NHS Test and Trace (which is part of DHSC).

Design objectives

The app has six user-benefiting capabilities that are designed to encourage mass download and daily use. These capabilities have been designed to meet the remit of breaking the chains of COVID-19 transmission and enable society to return to a more normal way of life.

Real-time high-risk area matches (alert)

The app will notify the user if the postcode district within the local authority changes risk level. The user will confirm their local authority once they have entered their postcode

district. The postcode district is the first section of the postcode (before the space). This facilitates alerts to users should the risk level in the selected local authority change.

Digital check-in diary (venue check-in)

The app will allow the user to check-in and check-out of venues that provide a QR code e.g. restaurants, shops and stadiums. If a venue later reports a cluster of positive coronavirus cases, the app user will be notified if they were present in the venue at the relevant time.

The remaining four categories are targeted at reducing public risk. These are:

Symptoms questionnaire (symptoms)

The app will allow the user to report their symptoms and the date when their symptoms started. Based on entering symptoms, the user will receive an initial indication as to whether they may have coronavirus. If the user's symptoms indicate they may have coronavirus, they will be asked to self-isolate and book a test.

Coronavirus test (test)

If the user's symptoms indicate they may have coronavirus the app will assist them in booking a test from the GOV.UK website. Once known, the test result will be provided in the app. Data entered used for the testing process is managed outside of the app environment and additional information is available elsewhere.

Where guided by current COVID-19 testing policy, the app user may be recommended to seek a confirmatory test. The app will provide advice to the user when this is necessary with appropriate signposting. The type of test is noted by the app and through the testing process. This enables the confirmation testing functionality and supports the purposes of the app.

The app provides an option to book a COVID-19 test in line with the latest testing and isolation policy. Where appropriate, an app user without displaying symptoms will be recommended to seek a COVID-19 test. This will include when recommended by Notifications in the app related to venues (somewhere the app user checked in) or digital contact tracing (another app user they were in contact with).

You can enter a test result in the app from testing mechanisms outside the app, not all of which require symptoms to be present. If the user is given a code during the process of getting a test, this code may be manually entered into the app so that the test result and test type can be stored in the app and the isolation count down adjusted accordingly.

As noted above, where an app users receive a positive COVID-19 test result but no onset of symptoms date is present, the app will prompt the user to enter one. This is in keeping with the objective to provide app user's guidance that accounts for other NHS advice about isolation periods.

When a new government significant testing scheme (either in England or Wales) are brought in at scale, the app will provide the user with the latest testing and isolation information and details. For example, these details include testing sites in your area and where to learn more about the particular scheme.

Self-isolation countdown (isolate)

The app will ask the user to self-isolate either because the user has reported symptoms indicative of coronavirus, or they have received an exposure notification (the contact case). Once asked to self-isolate, the user will have access to a self-isolation countdown which keeps a track of the time they need to spend self-isolating.

Helping the community (analytics)

The user will be able to help the public health response to COVID-19 by sharing information about coronavirus in the user's postcode district and local authority region and how well the NHS Test and Trace programme and App are working.

This design has been driven through the collection of the requirements and iterated through user research.

Further explanation of the functionality and processing that supports these 6 features is set out in this document. The app has been designed to protect the privacy of those who use it. Fundamental to this design has been the ICO Contact Tracing Principles – responses to these are summarised below.

ICO Contact Tracing Principles and app design responses

Be transparent about the purpose – explain if the current/future purpose is only proximity notification or broader

The purpose of the app is to enable society to return to a more normal way of life. To do this a combination of features are offered to reduce public risk by helping people:

- receive notifications if they have been near another app user who tests positive for coronavirus

- view current risk in the local area and receive a notification if there is a change that risk status

- keep a personal record of venues visited using the official NHS QR code and receive notifications if there is a reported outbreak at venues visited
- understand their symptoms
- be able to order a test, via a link to the NHS Test and Trace website
- have an easy way to track the days they are recommended to isolate (if required)

More detail is available in the introduction and design section of this document. The analytical data the app collects is to help manage the public health emergency.

The roadmap set out in this document illustrates current planning for future releases. The themes of new functionality relate to:

- maturity of app efficacy measurement via evolution of the GAEN
- evolution of testing options now including asymptomatic testing

For more detail, please refer to the section on the roadmap for future functionality of this app.

The purpose of the app is explained comprehensively in its associated privacy notice.

Be transparent about your design choices – use the least privacy intrusive approach possible. Explain risks.

The initial design for an NHS COVID-19 contact tracing app undertook a centralised approach to managing data, built around a clear focus on the epidemiological understanding of the disease.

With the Google Apple API (the GAEN) we have moved to a decentralised approach. This is a design that is the least intrusive to privacy as very little data leaves the phone and all matching happening only on an individual's device. Our commitment to transparency is further demonstrated by open sourcing our code, which was published along with the DPIA at the commencement of the early adopter phase.

Be transparent about the benefits – from both your perspective and that of the user. Explain how tensions between these are managed.

The 6 app capabilities have been designed for user benefit. Research has been undertaken with users to refine these capabilities.

One area of tension in the design is setting the risk threshold to determine the volume of people who are asked to isolate. This determination is based on the deemed risk of the encounter they have had.

The risk threshold is set taking into consideration the current reproduction number.

This value drives the number of people asked to isolate and is regularly reviewed.

This approach has been scientifically determined by the Alan Turing Institute. More detail is available below regarding Automated decision making and Article 22 (GDPR requirements).

Collect the minimum amount of personal data necessary – only collect or otherwise process information that is required for the core purpose (e.g. excluding location data).

The app has been designed to use the minimum amount of personal data possible. In all instances, the data required, used or stored is minimised to reduce or remove the ability to identify an app user and to maintain their confidentiality and privacy. As an example, information collected in the app includes the user's postcode district but as each postcode district is shared by ~8,000 households, this minimises the possibility of any personal identification. The user's area, both local authority and postcode district, is stored on the app. The user's local authority and postcode district are collected in the analytical data set, with controls to maintain the protections of privacy and identity.

More detail is available in the section 'nature of the data'.

Protect your users – use pseudonymous identifiers which are renewed regularly.

The app has no concept of registration, of allocating unique ids to app instances, or holding app instance specific data on the backend services.

Apple/Google exposure notification diagnosis keys are completely random and cannot be linked to the user. These are considered anonymous. A new diagnosis key is generated every day and will not be repeated. Diagnosis keys generate rolling proximity identifiers approximately every 15 minutes.

More detail is available in the section 'nature of the data'.

Give users control – ensure your users can exercise their rights.

The app has a section called 'About' which users can access to discover the information held about them. This information includes:

- postcode district and selected local authority
- venues captured via check in (if appropriate)
- last test result (if appropriate)

In a future release, this information might also include any symptoms entered by the user.

All data other than postcode district is able to be deleted from the app, with an option to the delete the postcode district available for update in a planned release. All data other than postcode district is able to be deleted from the app, with an option to the delete the postcode district available for update in a planned release.

Keep data for the minimum amount of time – explain what that period will be and why.

Diagnosis keys are kept for 14 days (the incubation duration for the virus). The keys are retained on DHSC secure computing infrastructure for a further 14 days. We will apply the same rationale to any diagnosis keys received from partner health service apps.

QR codes are kept for 21 days (this accounts for 14-day incubation period and 7-day infectious period of the virus)

The analytics data is anonymous as set out in more detail in Appendix 5, which explains how we ensure users cannot be identified from the analytics data from their app. More detail is available in section 'retention of data from the app'.

Securely process the data –apply appropriate techniques to secure the confidentiality, integrity and availability of data, both at rest and in transit.

The app system has been designed and developed in accordance with security principles that govern data on the device, data in transit, data processing on the backend.

More detail is available in section 'security of processing'.

Ensure the user can opt in or opt out without any negative consequences – functions decoupled to allow the user to benefit from one function without being compelled to provide data for others.

The features of the app do not have to be used, for example the user has the option to turn on venue check-in functionality to scan the QR code. Users are entirely free to choose whether or not to enter their symptoms or book a test.

The option to call 111 (or the appropriate equivalent) is available should the user wish to discuss their circumstances, or the advice they have received. Google and Apple have been keen to assess this position and are satisfied the solution does not contradict their GAEN, which does not track or directly / indirectly limit public access.

More detail is available in section 'overview of the functionality of the NHS COVID-19 App'.

Strengthen privacy, don't weaken it – do not introduce additional privacy and security risks for the user

We adhere to the principles which the Ethics Advisory Board set out for the first version of the app.

These principles are the basis by which any future change requests for the app will be assessed. Any request to add to or change the scope of the app will be formally presented to a Change Board which will convene weekly.

A core value of the app is privacy, specifically that the app must preserve the privacy of our users. In order to adhere to this value, the application and back-end service have considered privacy and security at each stage of design and development and has resulted in the use of a "decentralised" approach whereby data is stored and processed only on the user's mobile device.

An example is venue check-in. Users are encouraged (but not required) to scan QR codes on official NHS posters posted at venues. This simple act provides user-led control for privacy. In this instance, the QR IDs are only stored on the user's device and protected using encryption features available from their phone. The data never leaves their device, and can be deleted by the user at any time.

Where user identifiers are required, such as the virologic testing user journey, short-lifetime ephemeral tokens are used to protect the users' privacy.

The use of SaaS (Software as a Service) means that IP addresses of user devices may be logged by infrastructure components. The solution attempts to remove this association at the earliest possible opportunity. As a precaution, any IP addresses of users that are transmitted from the networking layer to the backend servers are ignored by the application (never collected, logged or stored), minimising the possibility of inadvertently recombining IP address and payload data. This is a key privacy enhancing control to support anonymisation of data held by the backend.

More detail is available in the section 'privacy by design and default', and section on 'security of processing'.

Information Commissioner's advice

The Information Commissioner raised a number of specific issues relating to the previous iteration of the NHS COVID-19 App, that are addressed in this document:

1. Data subject rights – see the section on subjects' rights

2. Automated Decision Making at Article 22 of the GDPR – see the section on automated decision making

3. Transparency requirements – it is intended that the app's functions will be clearly communicated using the material set out in the section 'design objectives'

4. Necessity and proportionality – see the section 'privacy by design and default'

5. PECR (the Privacy and Electronic Communications Regulations 2003 (as amended)) – including clarity of when information is stored on or accessed from user devices, and when opt-in consent is required. See the section on PECR.

Rationale for adopting the Google-Apple Exposure Notification (GAEN) API

See the section on 'necessity and proportionality' for an explanation of this decision.

Rationale for this data protection impact assessment (DPIA)

Data controllers are required by the GDPR to conduct a DPIA before introducing data processing which could pose a high risk to subjects in the absence of proper controls. In particular, when using new technologies.

DHSC does process personal data that relates to the health of a very large number of individuals, and there are new types of technology employed in doing this, but all have mitigations in place to substantially reduce risk.

The Information Commissioner's view is that organisations designing contact tracing apps are responsible for ensuring the app complies with data protection law. This is especially important because individuals may believe that the data protection by design and by default principles used in the development of the Contact Tracing Function extend to all aspects of a contact tracing app that is built to use it. Any supporting technology, including centralised processing to support contact tracing, should follow the same principles.

The app is designed to respect the privacy of those who use it. The identities of app users are not revealed as a consequence of its use. The App does not collect any directly identifiable information (for example, it does not collect name, telephone number, NHS number or GPS location data).

It is essential however to assure and formally document how the app works and how it protects the privacy of its users. Success relies on users' confidence in the information being processed by the app.

This DPIA supports the national rollout of version 3.3 of the NHS COVID-19 App. This document will continue to be subject to review and revision in light of ongoing insight and learning.

The nature of the data

It is essential to document the nature of the data and identify whether it constitutes personal data for the purposes of data protection legislation. The data dictionary is presented in appendix 1. Key features of constituent data items are referenced in the table above and described below.

The app makes use of the Apple/Google exposure notification system (hereafter the GAEN). This capability is incorporated in the latest versions of iOS and Android operating systems. The GAEN can only be activated when an authorised App is installed. The NHS COVID-19 App has been authorised for installation by the Apple and Google app stores.

The Google-Apple Exposure Notification (GAEN) API

The GAEN generates 2 types of identifiers:

- diagnosis keys
- rolling proximity identifiers (RPIs or broadcast codes)

Diagnosis keys

Diagnosis keys are generated by the GAEN and uniquely reference an instance of the installed app on a user's device. A new diagnosis key is generated by the GAEN every day and will not be repeated. Diagnosis keys are used by the GAEN to generate a further set of keys called rolling proximity identifiers (RPIs), or broadcast codes, approximately every 15 minutes (see below).

Diagnosis keys are released to the app when a positive COVID-19 test result is received. This is only possible with the express permission of the user. Once granted, they are submitted to DHSC secure computing infrastructure for distribution to all app instances.

Diagnosis keys (for a user who has submitted them) reside in the following locations:

- the GAEN of the submitting user's phone
- the app data of the submitting user's phone
- DHSC secure computing infrastructure
- the secure Federated Server used to support interoperability
- partner health service secure computing infrastructure in Gibraltar, Jersey, Northern Ireland and Scotland

- The app data of receiving users' phones
- The GAEN of receiving users' phones

Diagnosis keys are at no stage associated with any other information. The fact that they have been distributed for matching only indicates that the submitting user has been diagnosed as having COVID-19.

When distributed beyond the GAEN, diagnosis keys do not relate to an identified natural person. They also do not relate to an identifiable natural person by virtue of the design of the app and its supporting DHSC secure computing infrastructure – i.e. no identifying information is associated with them, technical controls are in place to prevent interception. On this basis they do not in themselves constitute personal data. This allows for their distribution without the need to disclose confidential patient information.

Diagnosis keys residing on the generating GAEN may be considered personal data by virtue of their association with the installed phone. The privacy design ensures that the controller cannot have access to these keys - other than for submission to the DHSC secure computing infrastructure.

Rolling proximity identifiers (RPIs)

The GAEN uses the daily temporary exposure key (TEK) to generate a new RPI approximately every 15 minutes. RPIs are made available over Bluetooth and are then collected by the GAEN running on other users' phones. They are also referred to as broadcast codes. RPIs are random and almost certain to be unique, with only a remote chance of being repeated.

TEKs or RPIs cannot be accessed by the NHS COVID-19 App without a user testing positive for COVID-19. The user must also give permission to release the keys. Once approval has been received, TEKs are provided to the App and deleted from the GAEN. They then become diagnosis keys. Only when diagnosis keys are known can the RPI be re-generated. RPIs are not considered personal data because they do not relate to an identified or identifiable person.

Exposure windows

The GAEN digital contact tracing uses Low Energy Bluetooth ("BLE") to approximate distance and duration of contacts between app users. Where 2 app users have been in contact, with the exchange of Rolling proximity identifiers (RPIs) or Broadcast codes, these measurements are used to calculate the risk of infection.

When an app user goes on to test positive for COVID-19 and chooses to share their Diagnosis Keys (an index case), their Diagnosis Keys are added to list of reference Diagnosis Keys provided to all app users. Should the GAEN detect a match, the process is

detailed above, the Exposure Window data set associated with the broadcast is used to determine if the app user should be alerted.

This Exposure Window data set and measurements of the interactions between users is used to calculate the risk of infection from the contact with the index case. The calculation creates a risk score from the risk algorithm. If the calculation results in a score above the set risk threshold, the app will issue an alert to the app user with advice and a recommendation (i.e. the user is recommended to self-isolate due to a risky contact).

For more detail on the Exposure Window and its use see the section 'Digital contact tracing: exposure windows'

Exposure Notification Alerts

As noted above, the GAEN functionality produces an alert when the risk score is above the risk threshold. These alerts are displayed as notifications to users and are designed to provide prompt public health advice.

To understand the impact of user notifications and to properly weight the data gathered by app users additional data items are being collected. These data items also address the ongoing technical concerns around the display of exposure notifications across all relevant phones and operating systems.

These data items enable the exposure notification function to be monitored. For example, changes in patterns of user acknowledgement act as an early warning of technical issues that need investigation. By understanding whether the user has paused the function, they can be discounted from any technical issues.

For the public health impacts of Exposure Notification, understanding how app users respond to alerts enables the data generated to be appropriately weighted when considering the public health learning and impacts of the service.

See the data dictionary, Appendix 1, for more information.

Postcode district

When the user installs the app, they are asked to provide their postcode district of residence. This is the first part of their postcode up until the space. Postcode district is uploaded to DHSC secure computing infrastructure daily with other anonymous analytics data.

Postcode districts are not regarded as constituting a component of the personal data in the data set when processed within the DHSC secure infrastructure, in the product or analytical data environments. This is due to the first level postcode district typically includes ~8,000 households, minimising the possibility of personal identification. There are

additional controls throughout the app's supporting systems, including the performance viewer, data flows to and data within the analytical environment which manage postcode districts which include a small number of households.

Local authority

When users enter their postcode district, they will be prompted to confirm their local authority. The selected local authority will allow users to get an accurate COVID alert level based on government restriction guidelines.

In future releases, a user's selected local authority will also be used to provide users with valuable information, such as the number of infections and tests within a specific local authority.

The Local Authority is collected as part of the analytical data set and is subject to the same standards and controls to remove the risk of re-identification. The risks of reidentification due to the collection of both Local Authority and Postcode District was considered and controls are in place to reduce and manage that risk.

See Appendix 5 for more information.

Test results

When a user is recommended to take a virology test, the server allocates them a short-lived unique token. This token is passed to the virology testing platform so that test results can be sent back to the app system. The token replaces the need for any personal identifiable information. The token is destroyed within 24 to 48 hours of test results being received.

The token is associated with fully identifiable personal data relating to the subject throughout the processing of the test. The one-time token and the test result are returned to the Cloud Services database which downloads them to the user's phone. The token and test result are then deleted. Test results constitute a component of the personal data held on the installed app. This is because the token relates to a user and is identifiable in the context of their use of the app. The test result and the token constitute pseudonymised personal data whilst they are held temporarily in the Cloud Services database. Test results which are uploaded to Cloud Services daily with other anonymous analytics data only include the test status - and not the token. They are not identifiable to a user.

This process differs for app user's utilising the Welsh testing system and website.

Personal data held only on the phone

The app processes data entered by the user about their symptoms in order to provide advice on isolation and signpost to testing services. The app will hold details of the users last test result, including the date, result and type of test. The type of test will determine if a

confirmatory test is advised, which is noted in the data held on the phone. Where required by the relevant testing policy, this data item is processed by the app's functionality to advice the app user about the confirmatory test recommendation. Where an onset of symptoms date is needed to provide isolation period advice, the app will prompt the user to enter one.

The app also collects QR codes from venues which the user has visited and checked-in to. Although this information does not leave the phone, the data does relate specifically to the user and therefore constitutes personal data. The app provides the functionality to delete this venue check-in details both for specific venues and as part of the delete all data held on the phone function.

Analytics data

Analytics data is collected by the app and submitted to Cloud Services specifically for the purpose of understanding the performance or behaviour of the app system. It is uploaded each day to Cloud services in anonymous form. Please see Appendix 5 for more information about this data and why we are confident it cannot be used to identify app users.

This Analytics data may include postcode district, test results and test type which constitute a component of personal data when held on the installed App on the phone. This is because they relate to a user and are identifiable in the context of their use of the App. Other personal data used by the App is only held on the user's phone and not part of the analytics data.

Symptoms data is not retained on the phone after submission in the analytics upload. This data is not considered personal data when held in anonymous form on DHSC secure computing infrastructure.

Area data, either postcode district or local authority, is not combined with symptoms data for the purpose of identifying where an individual is located. When the area is combined with other data items it is used for public health purposes, such as the monitoring of infection spread.

Data held on Cloud Services

Appendix 1 describes a summary of the DHSC secure computing infrastructure data. The server only handles data if it is needed for app operation or for system monitoring. No data held on the DHSC secure computing infrastructure is traceable to an individual. See below for details around the management of IP addresses.

Flows of Aggregate Data Derived from the NHS COVID-19 app

The app contributes data to the wider public health response to COVID-19 by providing data derived from analysis of app's data. This aggregate data is limited to the data processed by the app which is strictly necessary for the purposes of ensuring the app functions work. This aggregate data is provided to key parts of government to improve their response to the current public health emergency. Data is provided to a public dashboard as part of the commitment to transparency and to provide up-to-date information to the public.

The aggregate data provided does not constitute personal data and would not routinely be included within a Data Protection Impact Assessment as it falls outside the definition of personal data as defined by Data Protection legislation. We include a brief summary of the reason why we provide this data to the wider Department of Health and Social Care (DHSC), how we protect app user's data and maintain our commitment to protecting the privacy and identity of app users.

By choosing to download and use the app, members of the public are making an immediate and ongoing contribution to the response to COVID-19. App users benefit from the functionality of the app, including alerts and warnings of risk of infection, as well as enabling public health insight and responses. The app only collects data that is strictly necessary for its functions, to manage the service it provides and to ensure they are delivering public health benefits.

Aggregate data derived from the use of the app (we have used the term "aggregate derived data" in this document to describe this data) enables this analysis. Data that is strictly necessary for the functions of the app is collected as part of the daily analytical data set, events data set (exposure windows) and used to deliver and manage the functions of the app. After this analysis the insight and data that is produced enables a greater understanding of the transmission of COVID-19 and the public health response. For example, by determining how many app users are seeking to book a test (with a count being added to the daily analytical data set) the app can provide an early indication of both an increased demand for testing and potential increase in infection. This analysis validates the app's functions and the app's public health impacts to be assessed.

This information is disassociated from the specific app user. The app's aggregated derived data can be used by the DHSC's NHS Test and Trace programme to:

- Use aggregate data provided by the app alongside other data sets to target public health policy and inform decision making. For example, detect an increase in app users seeking tests or using the symptom checkers in different parts of the country;
- Provide key information to Local Authority Public Health functions;
- Target communications and resources to maximise the potential impact on the transmission of COVID-19.

In turn this contributes to the advice, alerts and support provided to app users. This is done whilst maintaining the commitments in this DPIA and associated documentation to app users and their data.

Use of this data is bound by:

- Obligations and commitments made in this DPIA;

- The terms of use for the Google and Apple's Exposure Notification (GAEN) technology;
- The Secretary of State's Ethical Framework for the NHS COVID-19 app;
- Ongoing oversight by the Department of Health and Social Care.

As part of providing this data, the risks associated with this DPIA were reviewed and updated.

You can find more information about the uses of data by these functions in the Privacy Notice for Test and Trace.

The data provided to the NHS Test and Trace Data Analytical Platforms (TTDAP) remains bound by the obligations of the app and ongoing oversight to ensure that this is the case. Oversight ensures that the aggregate derived data is used appropriately and in line with these commitments. It is aggregated and subject to protections such as small number suppression to further protect the identity of app users and prevent data being linked.

This enables them to provide better public health advice to Local Authorities, via CTAs and inform public health interventions by local teams.

Privacy by design and default

As described in the section above, the app has been built to respect the ICO's Contact Tracing Principles. Key privacy features of the app are that:

- users' identities will not be revealed by the app
- no persistent user identifiers will be processed
- the app will collect the minimal amount of data necessary
- as far as possible processing will take place on user's phone
- personal data does not leave the device without the permission of the user
- analytics data is only collected in anonymous form
- a performance view (via dashboards) using only aggregate and anonymous data to provide an oversight of the services provided by the NHS COVID-19 App
- there will be no third-party trackers gathering personal data in the app
- the user can delete the app and its data from their phone at any time
- data in the DHSC secure computing infrastructure will be made available only to individuals that have been formally authorised to access it
- transfer of data from the DHSC secure computing infrastructure to another system or controller, or processing for purposes outside the scope of this DPIA will be subject to further DPIA.

The app makes use of the Google/Apple GAEN, which is incorporated in the operating systems of Apple and Android phones. The features which ensure user privacy are outlined in this document.

Contacts, QR codes, local authority and postcode district data is processed on the device. Circuit breaker, diagnosis keys and anonymous data are processed off the phone.

The GAEN

The app is built upon the contact matching functionality of the Google/Apple GAEN. The GAEN is subject to routine review and improvement by Google and Apple based upon the what they have learnt about the technology, COVID-19 and the public health response. NHS Test and Trace has contributed to this discussion and undertakes vigorous testing to help understand and refine the risk algorithm used to calculate the risk of infection. The

most recent update introduced a second GAEN Mode, Mode 2, in addition to the existing Mode, Mode 1. A brief explanation can be found below.

GAEN Mode 1

When the GAEN receives a broadcast code they record a measure of distance, the BLE signal strength. Mode 1 takes the set of measurements it receives associated with the broadcast code and merges those signals into a three-bin histogram. This allows the GAEN to determine how many seconds the interaction was in the “near”, “middle” or “far” histogram bin.

Mode 1 allows signal information to be calculated into a broad categorisation of risk. However, the Mode does cause some uncertainty if the measure of distance (signal strength) is impacted by other factors. For example, the Bluetooth signal is muffled due to the device being in a pocket or bag. This is a challenge within indoor environments due the nature of Bluetooth and the impact on Bluetooth signals indoors.

Mode 1 is deemed “good” at identifying high risk scenarios, by the International Machine Learning scale. However, Mode 2 offered by Apple and Google offers greater ability to account for these challenges.

GAEN Mode 2

Mode 2 uses signal strength attenuation, the approximation of distance, as a function of time difference between successive Bluetooth measurements. Time difference and time series is the key new feature of Mode 2 which is enabled by the Exposure Windows functionality, and data set, which measures 30-minutes of interactions when broadcast codes are received by the app. These Time series are the signal strengths taken over successive intervals within the 30-minute period of an Exposure Window.

A better estimate of distance between app users can be calculated by using Mode 2’s time series of measurements. Before the app moved to use Mode 2, a series of experiments were done in a number of environments and settings to collect data and understand the performance of the app. This testing, and a review of the results by international experts and colleagues, allowed us to define the best possible algorithm for differentiating risks to ask only those at risk of infection to isolate. Read more information. The Risk Algorithm is open sourced and the NHS COVID-19 app is believed to have the best discriminative performance internationally.

On the International Machine Learning scale, the algorithm used by the app for Mode 2 is deemed ‘excellent’. For users this will result in fewer unnecessary recommendations to isolate.

Mode 2 is utilised by the latest version of the app and is another reason why we recommend app users to routinely update their app for the best service and performance.

Read more information about the use and processing of data by the GAEN Mode 2 and Exposure Windows. As with the GAEN, no identifiers are exchanged, and no personal data is processed due to the lack or removal of any possible identifiers of the individuals involved.

Stateless and conversational APIs

All of the APIs presented by DHSC secure computing infrastructure are either 'stateless' or 'conversational':

- stateless APIs do not save data generated in one interaction for use in the next interaction

- conversational APIs generate a token which is returned to the app in the initial communication allowing the app to poll for further communications relating to the same matter – this allows for processing to be conducted whilst the token remains current

Application Programming Interfaces (APIs) used by the app

APIs used to communicate with DHSC secure computing infrastructure are described below:

- Analytics – collects analytical data from the app for aggregation and statistical analysis (stateless)

    - Analytics – same API used for Event Analytical Data Set – Collects analytical data from the app for aggregation and statistical analysis (stateless)

- Config – provides configuration for the app, possibly based on device state, like language and type (stateless)

- Distribute – access the data used for risk scoring; positive diagnosis keys, hotspot QR codes and area (postcode district/local authority) risk levels (stateless)

- Risk – confirm with the DHSC secure computing infrastructure before taking a risk-based action such as isolation (conversational. The app request is returned a short-lived transaction ID. The token is needed as long as the circuit breaker takes to make its decision. There is manual input in this step, so time is not fixed. Rarely above 4 hours.)

- Submit – submit exposure diagnosis keys to be added to the positive key set (stateless)

- Control – support the control Panel web monitor (stateless)

- Swab testing – app-facing API used to get a transaction token and get the swab test results (Conversational. A transaction ID token is maintained while a swab test is underway, which is expected to be 1 to 4 days.)

- TestLab – 3rd party test lab API used by the swab test Labs to submit test results, together with the linking token ID. (Conversational. A transaction ID token is maintained while a swab test is underway, which is expected to be 1 to 4 days.)

- App Rest API client – collects and provides data to support operational interoperability with partner Health Service apps (stateless)

Supporting Isolation Payment Application APIs (please note: this may differ for Wales)

- TTSP Gateway API – supports the user's application in accordance with the app's privacy requirements (stateless)

- TTSP Mobile AP – creates and updates the token for the app user making an application (conversational, the transaction of tokens is confirmed)

All API interactions to the DHSC will inevitably result in app users' IP addresses being present in data communicated between the app and the DHSC servers due to the nature of networking. The DHSC will never use IP addresses for identification purposes. IP addresses are not processed and are removed as soon as is practical. The IP data is never held alongside data collected from app users.

No user account or registration process

There is no user account or registration process that requires the submission of direct identifiers. This includes no requirement (or opportunity) to submit name, email address or telephone number.

A central system, the DHSC secure computing infrastructure, is necessary to facilitate exposure notifications and the communication of test results. Use of the App does not however involve a persistent internal identifier to link data on the App with data in the DHSC secure computing infrastructure.

All communications between the App and the DHSC secure computing infrastructure database are conducted by polling rather than push notification. There is no need for a messaging service or messaging ID.

Distribution of data from the DHSC secure computing infrastructure database to the App is achieved by the App making requests to the relevant API.

QR codes for venues visited never leave the phone

A history of the scanned QR codes for venues a user has checked-in to is accumulated on the phone. This includes the This is used for matching against the distributed QR codes for venues identified as infected.

The codes scanned by the user never leave the phone.

The QR scanner is incorporated within the app to ensure that there is control over proper operation.

Details of the venue are encrypted with AES.GCM and the key is stored in private device key storage.

Analytics data is anonymous

App functionality which involves the backend (circuit breaker, key submission, onboarding) is real-time. Other analytics are collected on a regular basis, currently daily.

The analytics dataset is anonymous. As noted above, IP addresses of users when transmitted from the networking layer to the backend servers are ignored (never collected, logged or stored) thus minimising the possibility of inadvertently recombining IP address and payload data.

Performance viewer

Data from the NHS COVID-19 App's product environment is provided to those overseeing the performance of the app. This is based on the analytical data provided by app users as part of the analytical data upload. More details of the data items included can be found in the data dictionary in appendix 1.

The performance viewer is available to a limited number of staff within the Department of Health and Social Care's Test and Trace programme. Access is strictly controlled. Data provided to these viewers is subject to additional privacy and identity protections, such as small number suppression. The data supports data dashboards that provide those viewing the data with ability to question the data or change views. For example, they would be able to judge the uptake of the app within particular postcode districts or wider areas.

The dashboards and functionality are provided within the app's Product Environment, provided by Amazon Web Services acting as data processor.

Consent

Consent as a basis for lawful processing for GDPR purposes is not being applied.

Installation of the app is entirely voluntary; Specific permission is requested for the app to access Diagnosis Keys, for submission, and to open the camera to scan QR codes.

Location

The app does not use GPS or any other geolocation technology to collect information about the specific location of a user's phone.

The collection and recording of proximity encounters rely entirely on the strength of Bluetooth signals between communicating devices.

Security of processing

Threat modelling was conducted during the design stage. A STRIDE review was used to identify threats to data both in transit and at rest. These cover threats such as Spoofing, Tampering, Repudiation, Information disclosure (privacy breaches or data leaks), Denial of service and Elevation of privilege (STRIDE). Threats are prioritised based on potential or actual impact. All risks are covered, but threats remain unbounded.

Security principles have been established to define the controls needed to protect data:

Securing the systems that enable the app

Stateless microservices are used to deliver services where possible. The use of cloud provider services results in a highly scalable and reliable infrastructure.

All data is stored in encrypted storage.

Static data is monitored to detect change.

Service availability is continuously monitored as part of the operations function.

Securing data in transit

All data in transit is encrypted using TLS1.2+ using modern cipher suites.

Clients and services must mutually identify each other:

- the mobile device app provides an API key to the backend
- third-party services provide an API key to the backend
- the backend service presents a certificate that the connection initiator verifies is issued to the service (certificate pinning)

Data originating from the backend must be signed. Mobile app clients have a public key in the application which is used to verify the signature of data from the backend.

The infrastructure is protected through a range of techniques:

Architecture

Separation of environments – Environments are separated by use: development, testing, staging and production.

Use of DHSC secure computing infrastructure via cloud provider services – Where security functionality is available from the cloud service provider, these solutions have been selected over in-house or third-party solutions. These are proven services that are the responsibility of the cloud service provider to maintain. Where appropriate, we have followed the cloud service providers recommendations and guidance relating to secure configuration.

Use of microservices – Limited functions integrated into the SaaS architecture. Where possible these are stateless.

Use of web-based services – All web-based services use TLS v1.2 and all services require authentication (with the exception of requests from mobile devices where we attempt to preserve anonymity), and mutual authentication methods for service interconnects to other services are achieved where this is technically feasible using the chosen technologies

Repeatable delivery – The use of Infrastructure as Code is mandated to enable repeatable delivery of the environment and assurance of repeatability of test results.

These data flows support international travel whilst remaining protected under the international collaborative usage of the GAEN applications.

The solution is built and deployed into Public Cloud infrastructure, based upon Amazon Web Service (AWS) as a Processor, using combinations of Platform as a Service (PaaS) and Software as a Service (SaaS) components. Configuration and use of these components are under strict control by DHSC, but underlying operating environments are subject to change by the service supplier (AWS) to improve the security and resilience of AWS.

The performance viewer is hosted within the AWS instance that hosts the app supporting service. This allows it to provide visibility on the performance data received from the apps in real-time, not subject to delays that transfer to a separate environment would involve. The mobile apps send analytics information to AWS daily and when a test result is confirmed. The new exposure window information is triggered by the user entering a manual test result code or when they acknowledge a test result.

This data is made available to the performance viewer every minute. The presented dashboard data uses controls to prevent risks of indirect identifiability from the data presented.

This is implemented as an Amazon Kinesis Data Pipeline, which converts the data to a batch file format, writes this into Amazon S3/Athena, where it is then available as a reporting data source for Amazon QuickSight.

Traffic obfuscation techniques are implemented and maintained to reduce inference of communication content by ensuring random packet lengths and consistent sequencing of packets for different outcomes or user journeys.

System user management

Role-based access control – All users are granted permissions through roles. Access is granted on a per-environment basis.

Authentication – Multi-factor authentication is required.

The performance viewer presents data dashboards to entitled, authenticated users. The dashboards provide only read-only access to the app analytics. User authentication is achieved via the usage of role-based AWS accounts. The access restrictions for users of the performance viewer ensure that users are given permission only to view the information that is presented in QuickSight, and nothing further. Additionally at the system level the QuickSight processes are assigned AWS role policies that only allow access to the analytics data in the reporting data source, and no other system data.

Monitoring

Monitoring – Activities of highly privileged users and high impact actions are alerted in near real-time. These alerts are monitored by the app operations team.

Protective monitoring is described further below.

Test the effectiveness of the security measures and respond to any security issues

- Security measures are tested throughout the delivery lifecycle for both the applications and backend services:

- Design – Threat modelling is performed, prioritising threats and identifying suitable controls.

- Build – During deployment, backend security controls are explicitly tested to ensure that the configuration of the solution does not inadvertently lead to information leakage.

- Test – Active penetration testing is performed using an independent third-party supplier. Cloud service provider compliance services are used to verify that the service meets CIS recommendations.

- Operate – In addition to the ongoing performance of the activities described in the Test phase, protective monitoring is undertaken. To the extent possible, all source code is made available as open source, enabling anyone to identify potential security issues. Reports are encouraged through the HackerOne Vulnerability Disclosure Programme are triaged and responded to.

In addition to system protection, a number of components also detect compromise, significant events or compromise attempts:

- Protective security monitoring is deployed on the AWS platform and service running on the platform

- Proactive security alerting is implemented to notify when a privileged role has been used or a high impact event occurs

- Security logs are sent to the NHS Digital Cyber Defence Operations Centre (CDOC) for analysis of anomalous or malicious behaviour

- As a result of these alerts, security incidents are triaged by the incident management team who respond appropriately.

Protective security monitoring and application behaviour monitoring are provided by CDOC and a company acting under contract to the DHSC (Zuhlke Engineering). Zuhlke Engineering are not required to process any personal data and are not considered a data processor but operate under strict contractual controls.

Data flow lifecycle and data architecture choices

Data flows through the system have been described in relation to each feature in the section ‘overview of the functionality of the NHS COVID-19 App’.

The following principles have been used throughout the solution:

- no User State or Identifier is stored on the DHSC secure computing infrastructure

- all APIs are stateless where possible

- when stateful behaviour is required, short-lived tokens are used as identifiers. As described in the flow below this exist only as long as are needed

- some interactions are in place to support future functionality

- rich analytics are collected, protecting the app user's identity. For example, a user's IP addresses will not be recorded.

All web-service APIs owned by the project use TLS encryption and DHSC secure computing infrastructure require all app user's data to be embedded in the content of the payload.

The following data items are sent from the end user and stored in the DHSC secure computing infrastructure or persistent storage:

- diagnosis keys – A set of device keys encountered by the device. This data is only uploaded when the user has a positive test and they have specifically given permission to sharing through the app. If the user gives permission then this data is distributed to all devices periodically. The validity of the duration of the keys is defined by the Apple/Google API.

- analytics data – This is aggregated and made available for query by authorised users. This data is provided via dashboards for management and oversight of the service delivered by the app service. The data is also exported to the App Analytics Environment (AAE) for additional analysis and support of public health. interactions with the service which are logged through cloud provider services. These records are provided to the Cyber Defence Operations Centre to enable them to perform protective monitoring.

- venue check-in – registration for and provision of a QR code poster to venues that wish to display one outside of the scope of this DPIA. The process includes the email address and venue location. Where venue owners request a poster, they are required to provide an email address and location. This is used to send the poster to the individual registering the venue. A list of poster IDs and their associated location is provided to JBC.

The following data items from the end user are stored on the device and are not stored in cloud databases or persistent storage:

- symptoms submission (Not in use in the present version)

The following data items relating to the end user are stored on their device and are stored within back-end integrations with third parties:

- virology test bearer token – Where a user registers for a test, a temporary token is obtained from NPEx which is stored on the device and subsequently used to retrieve their test result (NPEx is a system owned and operated by Calderdale and Huddersfield NHS Foundation Trust in support of the national COVID testing operation)

Rationale for collecting postcode district

When the user installs the app, they are required to provide their postcode district. This is the first part of their postcode up until the space. On the EN Server this is included in the analytics dataset but is not considered personal data as it is fully anonymous.

The area, postcode district and local authority, are also used to provide app user's with details about the services in their area. For example, if there are any additional testing options.

The postcode district is collected in order to understand the geographical distribution of:

- app uptake
- reported symptoms of coronavirus
- potential transmission events

This data will be used to understand where the virus is spreading, and how fast it is spreading in different locations. This information could be used to coordinate local responses - be it by increased provisioning at the local NHS Trust or deploying more Test and Trace resources. The postcode district will also provide insight into regional variation in the uptake of the app as well as regional infection rates. The postcode district will also be used to alert users when their postcode district is at a higher risk from coronavirus.

Regional variation information will provide improved epidemiological insights. In future versions of the app, this information would allow the implementation of a localised risk function, including messaging within the app to provide users with information about COVID prevalence and services in their area. This could contribute to a more granular loosening/tightening of social distancing rules at a more geographically granular level. This would ultimately help to get more people back to normal life quickly and safely.

Rationale for processing local authority

When users enter their postcode district, they will be prompted to confirm their local authority. The selected local authority will allow users to get an accurate COVID alert level based on government restriction guidelines. The risk level will be presented in a manner that is compatible to the government guidelines to enable users to have an accurate risk level based on their selected local authority.

Confidential patient information

Diagnosis keys are an indicator that a referenced individual has become infected with COVID-19. If the individual were identifiable, then this would constitute confidential patient information for common law purposes.

Using or disclosing confidential information requires one of three bases for it to be lawful:

1. consent

2. overriding public interest

3. statutory permissive power or obligation

Diagnosis keys more precisely represent an approximate 24-hour period within which the EN API (operating on a user's phone) broadcasts rolling proximity identifiers (which expire and are replaced approximately every 15 minutes).

As neither the diagnosis keys nor the rolling proximity identifiers can be used to identify a user or their phone, they are not considered to constitute personal data away from the user's phone. Nor are they considered confidential patient information.

As described above, the receipt and communication of test results by the DHSC secure computing infrastructure involves the result being associated with a temporary one-time use token. The use of this code requires that it is associated with information that does reveal the subject's identity, such as name and telephone number – but only outside the app.

In the context of the DHSC secure computing infrastructure database, the token and the test result are transient. The only purpose being to facilitate communication to the user when requested by the app.

The token and the test results are considered pseudonymised, as no linkable identifying information is available to the controller. In order to provide maximum protection and privacy however, they will be treated as though they are sensitive personal data relating to health - and therefore confidential patient information.

Necessity and proportionality

At every stage of development, the intention of the UK government has been to adopt the technical solutions which support efforts to control the spread of COVID-19.

Initially, an app was designed which allowed for both effective contact tracing and provision of additional epidemiological functionality to manage the spread of COVID-19. The focus of this app was on collecting the minimum data necessary.

A new exposure notification framework was developed by Google and Apple however, which supported digital contact tracing through slightly different means. A review was subsequently taken to assess the Google/Apple API against the functionality judged beneficial for managing the spread of COVID-19.

The functionality of the Google/Apple API was assessed alongside rigorous testing of the original app. Testing revealed that reliability of the original app was not sufficient and would therefore not be effective in helping manage the spread of COVID-19.

The government decided that the Google/Apple approach had the highest likelihood of achieving the stated goals, while collecting the minimum data necessary. Following advice from his advisers, the UK Secretary of State for Health and Social Care, announced on 18 June that the government had begun the next phase of development in building a new app that supports the end-to-end NHS Test and Trace service. This app would use the Google/Apple decentralised exposure notification framework to achieve this goal.

The ICO opinion on the Google/Apple API is available

The roadmap for future functionality of this app

Improvements and enhancements within the functionality of the app go through a change control process, these adhere to the existing commitments to app users, accounting for information rights law and privacy requirements. This continues to be required and appropriate as the app responds to the developing public health emergency and identifies areas for improvement.

The scope of future functionality will continue to develop. New changes will always be subject to review based upon policy decisions and requirements. Many policy decisions will be for ministers to decide and cannot be pre-empted here. The following is under consideration for future release:

- the focus of the changes ahead in the app relate to being able to measure its efficacy which evolves as the Google Apple API matures (the GAEN). This direction and the specifics on the implications of data collected in an anonymous and aggregated manner are described in section on the risk threshold. These changes will come into effect across several releases over the coming months. No other major changes to functionality are currently expected

- updates to follow the testing path. The app was initially established to take testing results once a user has demonstrated symptoms. As additional testing options are

made available, the app looks to provide consistent advice, such as isolation periods, to all app users in line with the latest testing policy

The app is part of NHS Test and Trace and considers the broader roadmap for the whole programme.

Assessment of application of the Privacy and Electronic Communications Regulations 2003 (as amended) ('PECR')

We accept that regulation 6 is engaged as regards some portions of the app's functionality. These functions require access to data stored on the phone (for example performance metrics, diagnosis keys) and storing data on the phone (for example venue details, area (either postcode district or local authority) to support the associated alert function). All data that falls under PECR is deemed strictly necessary to provide services explicitly requested by the user.

The functions of the app that fall under the PECR are explained below (with further detail provided in the data dictionary set out in Appendix 1:

Performance and use metrics

To ensure the app is working as expected and that the user's phone can safely support the core functionality:

- contact tracing;
- venue check-in;
- symptom tracker;
- isolation status and reason;
- test ordering, status and process, and
- isolation support payments.

The app collects data items to enable these functions to be monitored and validated. This ensures that the app is operating:

- Accurately,
- Appropriately,
- Safely, and

- Securely.

For a list of the data items that support this purpose, see the Data Dictionary in Appendix 1 of the DPIA.

Medical device efficacy

To comply with accreditation requirements of the app as a medical device there is a requirement to collect information which demonstrates ongoing review of the app's efficacy as a medical device, providing full lifetime traceability that the medical features of the app are working properly – for example to cross check the swab test result levels with isolation advice to ensure the app's isolation advice is functioning correctly. This necessitates collection of data across the medical features of the app such as isolation status, swab test status and symptom questionnaire results.

Digital contact tracing

If the app user receives a positive test result, daily codes stored on the phone will be shared with other app users (subject to cryptography and referred to as Diagnosis Keys) alongside the onset of symptoms data but only if specifically authorised by the app user who has the positive test. To ensure this contact tracing and alert system functions safely and effectively, the app provides data in the analytical data set and event analytical data set about the user's postal district, exposure events and pause button usage. This data will be used to validate that the level of alerts users receive are consistent with the wider risk environment and is necessary to calibrate the efficacy of the alert system.

The Exposure Window data, with measurements of duration and distance of contact, are used in digital contact tracing to determine when an alert should be issued to the app user (i.e. the risk score is above the risk threshold).

Together with the relevant onset of symptoms data, which is used to calculate the infectiousness, the Exposure Window and Scan Instances data sets enable the app to calculate the risk of COVID-19 infection from a contact with an index case. For more detail about these data sets, see the section on Digital Contact Tracing: Exposure Windows.

Public health response management

To help public health authorities learn more about the virus and its transmission and take effective measures to manage the response to the COVID-19 public health emergency the following data are accessed from the app:

- postal district
- exposure events

- QR check in count
- symptom questionnaire results
- isolation status and reason
- swab test status
- pause button usage
- test result and test result pathway (i.e. what was the result of test and was it provided via the app or by SMS code)
- exposure window and scan instances of contacts with index cases

This information comprises the contribution app users commit to making when they download and use the app, to help support management of and response to the COVID-19 public health emergency. Sharing information about the efficacy of the NHS Test and Trace Programme (or the Test, Trace, Protect Programme in Wales) and app is critical to helping authorities understand whether the Programmes and the app are working as expected. It supports being able to learn and respond better to the public health emergency, thereby helping the community to stay healthy and save lives. The privacy and identity protections of the app ensure that app users can do this through anonymous data. Using these services helps reduce the transmission of COVID-19 ensuring that appropriate steps are taken. As outlined in the privacy notice for the app, the user has specifically requested to use these services and contribute by downloading and using the app.

Automated decision making and Article 22 (GDPR) requirements

We consider it is arguable as to whether or not Article 22 is engaged by the contact tracing function of the app. On one view, Article 22 might be said to apply where a user comes into contact with someone who has tested positive and so is advised by way of a notification sent via the app to self-isolate and order a test. It is noted that in order for Article 22 to apply, there must be a decision that has a legal or similarly significant effect on an individual that is based solely on automated processing of personal data.

In any event, whether or not Article 22 applies as a matter of law, in order to try and maximise the ICO's and the public's confidence in the app, we have decided to take all the relevant steps and implement all the appropriate protections to comply with Article 22 as if it were engaged. We are taking all steps required to comply with these requirements.

For the purposes of its effective compliance with the requirements of Article 22, DHSC considers that any automated decision making is authorised by law, specifically section 2A of the NHS Act 2006 which permits the Secretary of State to take such steps as he considers appropriate for the purpose of protecting public health. This is the power that the Secretary of State relies on to authorise the design, implementation and operation of the App by DHSC. We have also sought to implement suitable measures to safeguard the data subject's rights, freedoms and legitimate interests as would be required by Article 22. As regards Article 22(4), we note that any automated decisions based on special categories of personal data shall be processed on the basis of Article 9(2)(g) being processing that is necessary for reasons of substantial public interest, following the conditions in paragraph 6 of Part 2 of Schedule 1 of the Data Protection Act 2018 (Statutory and government purposes).

See our document on processing of special categories of personal data.

Informing the app user

Upon downloading the app, the user will be informed that the app's contact tracing function includes a type of automated decision making.

Support and advice 111

When a user is receives a notification to the effect that they should self-isolate, they will be able to call NHS 111 to discuss the implications of this advice and their personal circumstances.

This will be particularly helpful, for example, should an individual receive a notification despite the fact that they have not been in direct contact with anyone for an extended period. The user would be able to discuss these circumstances with the NHS 111 operator who might advise that self-isolation and ordering a test is not necessary.

For app users in Wales, they will be directed to the equivalent service in Wales (see https://111.wales.nhs.uk/ for more information)

Circuit breaker

The 'circuit breaker' is a backend feedback and control service. It enables the app to manage notifications by the app where there are concerns about accuracy or where a significant number of app users may be told to self-isolate.

The circuit breaker triggers automatically when conditions are met. These conditions are set by human intervention and stop exposure notifications from being sent. Two examples of where this may apply are:

- Concerns over accuracy of testing results or data (referred to as compromised)
- Concerns over venue notification

The functionality will not be utilised in the initial release of the app. A review of the processes and criteria for intervention will be undertaken during this period by the Public Health functions responsible for the intervention

We look forward to continuing to discuss the above with the ICO, and particularly whether any further proportionate additional measures could be implemented for the benefit of App users.

For further context on contact tracing functionality, we set out below how we arrive at the risk threshold for recommending self-isolation.

Risk threshold for isolation

The app uses GAEN to measure Bluetooth Low Energy (BLE) signal attenuation— device calibrated received signal strength between transmitting and receiving smartphone devices. The API defines 2 user types: affected users (those that have tested positive) and potentially exposed users (all other app users).

The GAEN functionality now provides two Modes, see section on GAEN Modes for more information. Depending on which version of the app you are using, the relevant Mode and risk algorithm will apply. We recommend all app users to routinely update their app to get the best service and support. The risk threshold for the app is under regular review and may change. This is to ensure that the app alerts users in line with wider public health policy, ongoing learning about the performance of the digital contact tracing and app.

To identify the impact of different risk threshold settings, the team from the Alan Turing Institute used statistical modelling to generate data for 100,000 simulated encounters. In order to calibrate the statistical model, experimental data from Massachusetts Institute of Technology (MIT) was used. MIT have has run a series of real-life scenarios conducted in a controlled environment where device signal attenuation and precise distance have been recorded. The statistical model was then used to generate 100,000 known encounters, enabling an understanding of whether the app would categorise these encounters as risky or not.

From this, the modelling compares the numbers of true positives (correctly identified as high risk), true negatives (correctly identified as not at high risk), false positives and false negatives, for different risk thresholds. This is the scientific basis of the app's automation to recommend an app user to self-isolate. We have also researched the approaches being taken by Denmark, Italy, Germany Switzerland, Ireland and Northern Ireland, where a difference can be observed in aligning the likelihood of more false positives or more false

negatives. Read more information on the risk algorithm and ongoing work to improve it and Updates to the algorithm underlying the NHS COVID-19 app .

Setting the risk threshold

Based on the understanding of Mode 1 and Mode 2 API, because we use Bluetooth Low Energy (BLE) signal strength, it is not possible to definitively identify all the high-risk encounters between app users. Consequently, a judgement is made on the risk threshold to ensure we maximise the number of high-risk encounters identified without including too many lower or medium risk encounters.

Various factors impact on the decision to set the risk threshold, these include:

- changes to the risk algorithm, for example if Google and Apple introduce more capabilities
- analysis and testing provide more insight on where the risk threshold should be set
- where the COVID-19 public health situation and its impacts require a review

Ongoing field trials of the app, modelling and simulation are used to constantly evaluate the real-life behaviour of the app.

The Early Adopters phase of the app used the GAEN Mode 1. It considered the distance and duration of encounters. Modelling was undertaken to estimate the ability to maximise the number of high-risk encounters identified and minimise the number of lower or medium risk encounters that might be mistaken for high-risk encounters. The risk threshold was set accordingly.

The app forms part of the wider Test and Trace programme, which includes manual contact tracing, which is at the core of public health management and which the app's digital contact tracing compliments. Manual contact tracing can mitigate this risk to a degree as contacts, who are known to the index case, will be identified through the manual contract tracing process. The other factor in setting the risk threshold was to minimise the number of app users asked to isolate unnecessarily.

On 3 occasions since the early adopter phase, based on further modelling, we have adjusted the risk threshold. Based on insights from modelling and updating of the algorithm, we have been able to lower the risk threshold, yet maintain the same accuracy for high risk interactions. This has allowed us to reduce the number of isolation alerts sent unnecessarily.

Risk Algorithm – Calculating the Risk of infection

Five factors are used to calculate the risk of infection from a contact between app users.

The following factors are approximated by the GAEN and used by the app to determine the risk of infection from contact with an app user with COVID-19.

- infectiousness of index case at time of encounter
- distance related factor
- duration related factor

Two factors are set as a default for app users as part of the privacy protections in place and limitations of the technology (BLE).

- Weighting associated with potentially affected user (e.g. age)
- Context adjusting factor (e.g. indoors / outdoors)

Whilst these two factors are important the app does not account for them and they are set to a default that is the same for all app users and contexts, as the app cannot determine whether you are indoors or outdoors. An index case is an app user who has tested positive for COVID-19, updated their app and chosen to share their diagnosis key. Their infectiousness is calculated from the onset of symptoms data which, where available is provided along with the diagnosis keys. Our understanding of the virus that causes COVID-19 is that infectiousness is at its maximum as symptoms are about to start. Providing the onset of symptoms data alongside the Diagnosis Key allows this to be factored into the risk calculation.

Links

Risk score is a combination of these factors, as detailed here.

Use of the app by children

The app will be available to children between the ages of 16 to 18. We refer to these as young app users. The existing features of the app and messaging are appropriate for young users. We have undertaken user research and engagement with key stakeholders. We have also used the ICO's age Appropriate Design Code to support our design choices. To help mitigate any potential risk of self-isolation advice or a copy of test results causing anxiety for young users, alerts have been adapted for all users to include text that if they are under the age of 18 they are advised to show the message to a trusted adult.

All app users will be supported by links from the app to details about other services in the NHS Test and Trace programme, in England, and those determined by NHS Wales Informatics Service (NWIS), in Wales.

All app users are asked to confirm is they are 16 or over during loading of the app. This is a manual confirmation with no external validation. The response is not collected. If the app user confirm they are under the appropriate age for the app they will receive an appropriate message and be unable to continue using the app.

Necessity and proportionality

We revisited the necessity and proportionality review undertaken for older app users in light of the app's use by young app users. Our conclusion was that processing is in the best interest of the young app users. The app is a key part of the country's ongoing COVID-19 response, aiming to extend the speed, precision and reach of the existing NHS Test and Trace service.

The app has been trialled for early adopters aged 18 or above. There are approximately 1.3 million 16 to 17-year olds across England and Wales, with access to smartphones.

Extending the availability of the app to users aged 16 to 17 years:

- provides access to information and potentially notification of exposure in their day-to-day lives which they can use to protect themselves and others;
- allows young app users to benefit from the features of the app to reduce their personal and public risk, helping control the spread of the virus;
- enable them to engage with every aspect of the NHS Test and Trace service, from ordering a test through to accessing the right guidance and advice;
- access the functions of the app and support the government's management of the COVID-19 public health emergency

Additional data flows and data items collected about young app users

There are no additional data flows or data items associated with young app users.

Privacy notice for young app users

The privacy notice for the app will account for young app users either within the existing document or in supplementary material and will be published.

Privacy risks for young app users

The controls of privacy risks in place to protect all app users are equally applicable to young app users. The app is not considered to pose additional privacy risks and safeguards are in place to allow the deletion of data held on the phone. This includes the ability to delete specific venue check-ins. Notifications with self-isolation messaging advise

users under 18 to show the message to a trusted adult, it is up to the young app user to decide if this is appropriate.

Privacy risks, controls and mitigations are under ongoing review to ensure that they are appropriate and robust.

Age appropriate code

We have adhered to the principles set out in the Information Commissioner's Office age appropriate design code for young app users.

Privacy and Electronic Communications Regulations (PECR)

There are no additional considerations with respect to young app users for PECR.

Automated Decision Making (GDPR, Article 22)

As noted in the section Automated Decision Making, we have decided to take all the relevant steps and implement all the appropriate protections to comply with Article 22 as if it were engaged.

Recital 71 states that automated decision-making within the definition of Article 22 should not concern children. However, this is not a prohibition. It is considered that the essential contact tracing function of the app and advice for users to self-isolate should apply to 16 and 17-year-old users in the same way that it applies to adults.

For the purposes of its effective compliance with the requirements of Article 22, the measures put in place to safeguard the rights of adult users will also apply to young app users Notifications to the effect that any user is advised to self-isolate include the message that users under the age of 18, are advised to show the message to a trusted adult.

In accordance with section 2A of the NHS Act 2006, any use of automated decision making here is justified as it is appropriate for the purpose of protecting public health.

Working with other health service digital contact tracing apps (interoperability)

To further disrupt the spread and transmission of coronavirus (COVID-19), several jurisdictions are working together to deliver Exposure Notifications where an app user has moved between jurisdictions or app users from different jurisdictions have interacted.

As all the relevant apps are using the same digital contact tracing, the GAEN, the functionality can support app users across jurisdictions whilst still protecting their privacy

and identity. This process will involve sharing of Diagnosis Keys between these jurisdictions subject to controls, assurance and ongoing oversight.

The jurisdictions currently involved are:

- Within the Common Travel Area: i. Northern Ireland ii. Scotland iii. Wales iv. England v. Bailiwick of Jersey, which is a British Crown Dependency, as part of the Channel Islands

- Additional jurisdictions:

i. Gibraltar, which is a British Overseas Territory

It is intended to include Republic of Ireland, which is part of the Common Travel Area, as soon as is appropriate. The jurisdictions have adopted an Interoperability Agreement.

This agreement sets out the expectations and obligations on each jurisdiction and how they intend to deliver this support for app users. There are additional written agreements and controls to support the appropriate, accurate and secure transfer of diagnosis keys between those jurisdictions.

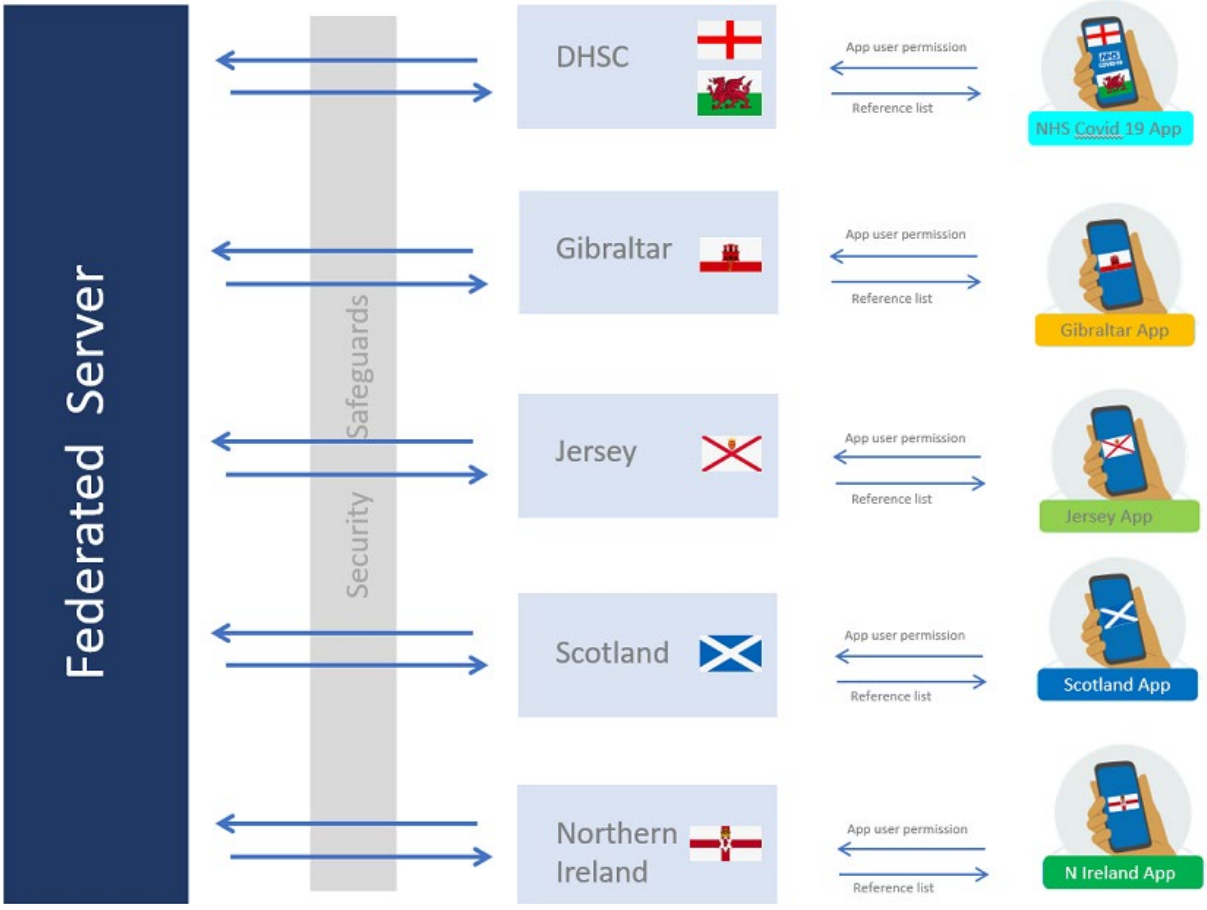


Fig 2. Overview of Interoperability diagram

Necessity and proportionality

The provision of interoperability supports the necessity and proportionality argument for the app and its use of data. By providing anonymised diagnosis keys to other jurisdictions we maintain the privacy of app users while supporting appropriate health alerts. What will be shared is the minimum data necessary to support interoperability. See section necessity and proportionality for more information

User choice (within the NHS COVID-19 app)

As set out within this DPIA, when a user receives a positive COVID-19 test result and their app status is updated, they are prompted to share their diagnosis keys. If they give permission, these diagnosis keys are submitted to the central system where they are added to the list of diagnosis keys provided to all app users. Users will be informed that we will provide their keys to the other locations as listed to support the digital contact tracing across jurisdictions.

The use of the data will support the purposes of the digital contact tracing functionality and response to the COVID-19 Public Health emergency across these jurisdictions. It will be subject to the controls in use by each jurisdictions and obligations owed to app users.

Data subject rights

There are no impacts on data subject rights arising from interoperability. However, the NHS COVID-19 app is committed to be fair and transparent with app users. We will communicate interoperability to its app users through the app, the privacy notice and by providing details within the Data Protection Impact Assessment.

Additional processing to support Interoperability

In addition to being provided to all NHS COVID-19 app users in England and Wales, as part of a set of reference data, that the app uses to assess whether a user needs to be alerted to an increased risk, interoperability requires the following additional steps:

- each jurisdiction will upload their diagnosis keys to a federated server
- each diagnosis key is associated with a type of test, enabling each partner to apply the testing and isolation policy for their area
- each jurisdiction will have a distinct area within the federated servers for the keys they upload
- analytics support the service to validate the processes and ensure accurate and consistent use of diagnosis keys across partners

- they will ensure that the diagnosis keys are submitted securely from each jurisdiction and can then be made available to other jurisdictions

- jurisdictions within the interoperability agreement will download Diagnosis Keys from Federated Servers on a regular basis to their app support systems. For the NHS COVID-19 app these systems are detailed in this DPIA

- the diagnosis keys are then provided to each jurisdiction's app users as part of their existing Digital Contact Tracing via the GAEN functionality

- The process preserves the privacy and identity of app users from each other and from the government's providing the service. Further details are available in each jurisdiction privacy information.

- storage of the diagnosis keys from the Federated Server will align with broader retention for each app

- The NHS COVID-19 app retention of diagnosis keys is detailed in the section on retention and we will keep all Diagnosis Keys for period noted.

As noted elsewhere, no IP address will be submitted with the diagnosis keys to the Federated Server by any party. Controls within the NHS COVID-19 app for the removal of IP addresses can be found in this DPIA.

Processes will ensure that the diagnosis keys are made available to other jurisdictions in a format that supports digital contact tracing and accounts for changes to the GAEN or associated Operating Systems.

Processes will ensure that the diagnosis keys are made available to other jurisdictions in a format that supports digital contact tracing, accounts for different test types as well as changes to the GAEN or associated Operating Systems.

In addition to the diagnosis keys, jurisdictions will work to together to ensure that the systems are safe, secure and accurate. This will involve providing data to support appropriate oversight, testing and isolation policy can be applied, access controls and technical requirements such as synchronisation. These are not derived from app users or related to the Diagnosis Key but would for instance, indicate the number of diagnosis keys submitted by each jurisdiction each day. These analytics do not relate to app users, or meet the definition of personal data, as no partner jurisdiction can identify an individual from them.

In order to support the use of digital contact tracing apps based on the GAEN across jurisdictions, work is underway to assess and minimise the amount of data required. As additional partners are considered, the potential amount of data from providing diagnosis

keys may increase. In order to reduce the cost or impact on an app user's data allowance whilst travelling, we are looking to minimise these impacts. For example, only providing app users with diagnosis keys submitted from jurisdictions that are relevant to them. Further work is underway in this area.

Interoperability assurance and oversight

Though diagnosis keys are considered anonymous data items, the supporting assurance and technical oversight will manage the data to the standard expected by GDPR. This will include ongoing governance, an agreed technical protocol between all parties and an ongoing process of testing and assurance. This will cover the federated server(s) used noting requirements for business continuity and disaster recovery to ensure a consistent and predictable service between parties.

Legal Basis for providing this service in England and Wales

The Secretary of State for Health and Social Care has powers to protect public health which include the provision of mobile applications; this is underpinned by section 2A of the NHS Act 2007 which provides the power. The processing of diagnosis keys is strictly necessary to delivering health care to app users.

Welsh Ministers entered in an agreement with the Secretary of State for Health and Social Care under section 83 of the Government of Wales Act 2006. This agreement covers the provision of a Contact Tracing Application, the NHS COVID-19 app, in Wales.

Providing alerts from Contact Tracing Applications, utilising the same GAEN functionality, supports these legal duties towards citizens and enables:

- the appropriate management of public health incidents
- the issuing of advice and guidance to members of public to enable them take appropriate action and seek clinical interventions

For interoperability, these diagnosis keys will only be relevant where:

- The app user has interacted with an app user from another jurisdiction
- The test type supports the testing and isolation policy of England, Wales or the partner health service
- The functionality of the app determines that it is appropriate for the user be alerted

Details of the process for this app can be found in this DPIA and published material.

Compliance with information law

Whilst the data shared with other jurisdictions is considered anonymous, the following assessment was undertaken.

The sharing of the diagnosis keys with other jurisdictions supports the following purposes and functions of the app.

Purposes

- Digital Contract Tracing
- Receive notifications if they have been near another app user who tests positive for coronavirus (when appropriate)
- Driving safer behaviour by helping people manage their risk exposure
- Identifying and alerting known and unknown contacts when transmission may have occurred

Function (as relevant to PECR)

- digital contact tracing (relevant to PECR)

The relevant key objectives of the app, supported by interoperability, include:

- create an enduring new medical technology to manage public health
- promote behaviour change by helping people manage their risk exposure
- identify and inform people to help communities manage public health emergencies

GDPR Article 6

Where personal data is processed by the NHS COVID-19 app, the following lawful basis applies:

- GDPR Article 6(1)(e) – the processing is necessary for the performance of its official tasks carried out in the public interest in providing and managing a health service

Interoperability through Diagnosis Keys, noting the key is not personal data as defined by GDPR, is in line with this basis for processing.

GDPR Article 9

Where special categories personal data is processed by the NHS COVID-19 app, the following lawful basis applies:

- GDPR Article 9(2)(g) – the processing is necessary for reasons of substantial public interest in the basis set out in Part 2 of Schedule 1 of the Data Protection Act 2018 (para 6 (Statutory and government purposes))

- GDPR Article 9(2)(h) – the processing is necessary for medical diagnosis, the provision of health treatment and management of a health and social care system

- GDPR Article 9(2)(i) – the processing is necessary for reasons of public interest in the area of public health

Interoperability through diagnosis keys, noting the key is not personal data as defined by GDPR, is in line with this basis for processing.

Automated Decision Making (ADM), GDPR Article 22

There are no additional considerations with regard to ADM with the inclusion of Diagnosis Keys from other jurisdictions.

Privacy and Electronic Communications Regulations (PECR)

Regulation 6 of PECR governs the use of data; there are no additional requirements as a consequence of interoperability and sharing of Diagnosis Keys. As noted, the use of this data is strictly necessary for the Digital contact tracing detailed in this DPIA.

Data Protection Act 2018, Schedule 1

Where special categories personal data is processed by the NHS COVID-19 app, the following lawful basis applies:

- DPA 2018 – Schedule 1, Part 1, Section 2(2)(f) – the management of health care systems or services

- DPA 2018 – Schedule 1, Part 1, Section 3 – public health purposes

Interoperability through Diagnosis Keys, noting the key is not personal data as defined by GDPR, is in line with this basis for processing.

Common Law Duty of Confidentiality

The diagnosis key, as it is associated with a positive COVID-19 test for an app user, will be treated as if a common law duty of confidentiality is owed when used by the NHS COVID-19 app. This is regardless of the point of origin of the diagnosis key. See the section on 'confidential patient information' for more information.

Human Rights Act

With regards to the right of privacy, Article 8, interoperability contributes to the objectives and supports the protections of privacy. Further Human Rights considerations of interoperability are in line with the broader assessment and purpose of the app.

Retention of data from the app

Diagnosis keys are retained on the user's phone for 14 days and are then deleted (14 days is the incubation period for the virus). Submitted diagnosis keys are retained on the DHSC secure computing infrastructure for 14 days and then deleted. So, the maximum age of a diagnosis key that has been distributed to DHSC secure computing infrastructure is 28 days.

QR codes that are scanned by the user when visiting venues are automatically deleted after 21 days. This is to take into account the 14-day incubation period, and 7-day infectious period of the virus.

The retention period for analytics data is subject to confirmation. As the data is anonymous, GDPR Article 5(e) which requires that personal data is kept in identifiable form for no longer than is necessary, is not engaged.

Retention of data sets outside of Data Protection Legislation

Data submitted by app users will not contain direct, indirect or consistent identifiers meaning that retention should not be considered in the context of GDPR. However, retention of data sets and records needs to be set even where it does not constitute personal data. This applies to the analytical data noted above.

Retention of records associated with the app are likely to fall into 2 categories, records which are used to:

- hold organisations to account is held for 8 years;
- monitor communicable diseases, for example in the COVID-19 Public Health Emergency, are retained for 5 years (if they contain personal data which is not the case in this instance) and 20 years for anonymous data prior to any review

Retention for these records is governed by the relevant Section 46 Code of Practice, Public Records Act and statutory duties of the organisations accountable (the Department of Health and Social Care).

Subjects' rights

Data held on DHSC secure computing infrastructure

As described in the section above, the personal data processed on DHSC secure computing infrastructure (i.e. the test code and test result) does not enable identification of a data subject by the controller. In order to respond to a subjects' rights request DHSC would need to associate additional information with the data held. This would undermine the privacy controls that we have incorporated.

Under GDPR Article 11(1) a controller is not obliged to maintain, acquire or process additional information for the sole purpose of complying with the Regulation – e.g. responding to subjects' rights requests. On this basis we will respond to requests made in relation to data held on DHSC secure computing infrastructure that we are unable to provide the information as the exemption in Article 11(1) applies.

Data held on the phone

Subject access and right to erasure

We have discussed in previous versions of the app the importance for individuals to exercise their rights, specifically the right to access the information held about them.

The methods for 'Managing my Data' are described in the Frequently Asked Question (FAQ) document available here. [What does the Manage My Data section of the app show me? · COVID-19 app support]

This user flow is displayed below. These screens may slightly differ from those actually within the app.

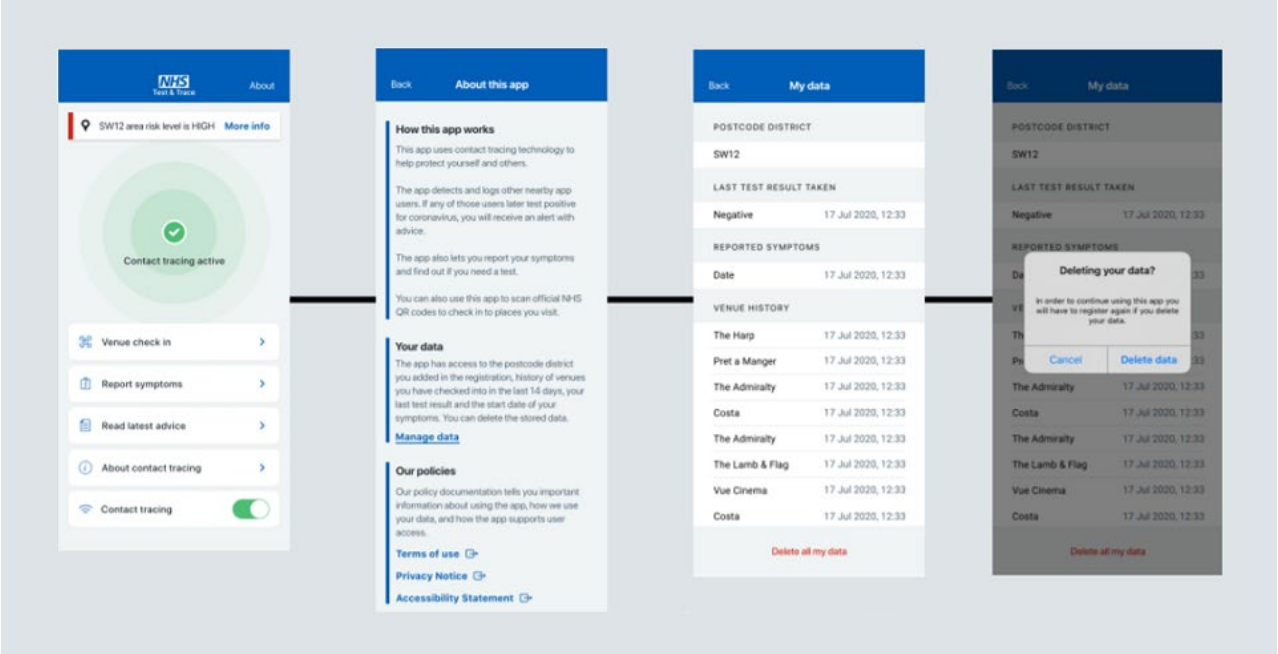


Figure 3. Subject access and right to erasure user flow

Users may also uninstall the app at any time, at which time all the data held on the phone is erased. Should the user have submitted diagnosis keys these will be deleted from the DHSC secure computing infrastructure database within 14 days as a matter of routine.

Subjects' rights - summary

How will you action requests from individuals (or someone acting on their behalf) for access to their personal information?

Subject access requests will be facilitated by a feature of the app to present personal data held in the App on the phone. This will include: the postcode district you have entered, the local authority you have selected, the venues you have captured via the check in, symptoms onset date and your most recent test result.

No personal data can be retrieved from the DHSC secure computing infrastructure database. As above, this is only the test code and result, and the exemption in Article 11(1) is engaged.

How would you locate all personal data relevant to an individual?

All personal data that can be provided to app users will be on their phones.

What is the procedure for this system to responding to data subject's request to be forgotten – Article 17

Users can delete the personal data associated with the venues they have checked into and their most recent test result. They may also uninstall the App from their phone at any

time which will cause deletion of all personal data from the device. As noted above, new functionality allows app users to delete individual venues from their phone.

Personal data will not cascade to the DHSC secure computing infrastructure database. The diagnosis keys are deleted after 14 days automatically. However, diagnosis keys away from the user's phone are not considered personal data

Article 16 – Right to rectification

Not available – controller does not have access to the personal data on the phone. If a user disagrees with a test result, they will need to contact the test provider.

Article 18 – Right to restriction of processing

Not available – controller does not have access to personal data on the phone.

Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing

Not available – controller does not have access to personal data on the phone.

Article 20 – Right to data portability

This right is not available because the processing is not based on consent pursuant to Article 6(1)(a) or Article 9(2)(a); or on a contract pursuant to Art. 6(1)(b).

Article 21 – Right to object

Available by uninstalling app. As well as the choice to use functionality, such as the venue check-in, and the ability to delete the data held by the app.

Article 22 – Automated individual decision-making including profiling

See discussion above.

Human rights

Human rights are a key consideration for an app that may involve millions of users and the management of the COVID-19 Public Health emergency. However, the advice to app users are not enforced by the app and are set by broader Public Health Policy. A human rights review has been carried out by the programme and is summarised here.

Whilst the ECHR and HRA does not enshrine rights as absolute, especially in the context of a public health emergency and pandemic, the app continues to uphold those rights and where possible support them in the context of COVID-19.

Rights that have been considered include:

- ECHR Article 8 – respect for private and family life
- ECHR Article 5 – right to liberty
- ECHR Article 2 – right to life
- ECHR Article 11 – right to freedom of association
- ECHR Article 9 – right to freedom of religion
- ECHR Article 14 – prohibition of discrimination

Workstreams to support human rights obligations and agenda include:

policy, strategy and communication work streams that directly address, consider or contribute

the equalities and health inequalities work, related to the DHSC legal duties under the relevant statutes and various policies

Public health purposes and value of the app

The app is intended to influence the behaviours of a proportion of the public sufficient to alter the trajectory of the COVID-19 outbreak. By providing alerts and monitoring app users' proximity to those who present a risk of infection or may be at risk of infection, this is intended to alter the behaviour of a proportion of those groups.

The app will give citizens maximum freedom with minimal risk during a public health emergency by:

- driving safer behaviour by helping people manage their risk exposure
- identifying and alerting known and unknown contacts when transmission may have occurred
- enabling users to isolate and test to reduce transmission
- supporting and informing users during isolation
- creating an enduring new medical technology to manage public health emergencies

In doing so, it will contribute to the objective of the Test and Trace programme: breaking the chains of transmission by minimising the frequency and extent of the COVID-19 outbreaks, to enable society to return to a more normal way of life.

The app will also provide information to support the tactical and strategic management of the COVID response.

Overview of the functionality of the NHS COVID-19 app

Each of these features is summarised below, including overall description, pointer to the appropriate user journey in the relevant annex, summary of data flows, list of requirements gathered which determined this feature.

User flow diagrams for each of these features can be found in annexes 1 to 6 of the data protection impact assessment.

Digital contact tracing: Exposure Windows

Introduction

As Apple and Google continue to improve their digital contact tracing system (the “GAEN” or Google Apple Exposure Notification) there is an increased ability to process data to support the purposes of the app.

With the latest changes, Google and Apple can provide the app team with more detailed technical data. The work done so far, the testing undertaken by the app team, and the analytical data set, has allowed the risk algorithm used by the app to be improved.

This allows the app to more accurately identify when an app user is at risk of infection and when they should isolate. Work undertaken by the app’s data science team was shared and checked with colleagues around the world. This has improved the risk algorithm we use, that is used to generate a risk score and the risk threshold. See the section on risk threshold for more information.

We have continued to carefully consider the potential impacts on privacy and risk of any change, such as the risk of reidentification, the app continues to preserve the privacy of the app user. The app will never and cannot track you.

This refinement, utilising Mode 2 of the GAEN, is an improvement but the extra detail available in the Exposure Window set will help:

- evaluate how the app is working
- what impacts the app is having on the chains of transmission of COVID-19
- what we can learn about the infectiousness of the COVID-19 from the data provide by app users

These are processed by the GAEN as part of the Exposure Window functionality and associated data sets, the “Exposure Windows” and “Scan Instances”. Apple and Google have made these data sets available to those using their digital contact tracing including the NHS COVID-19 app.

GAEN Mode 2 and the Event Analytical Data set of Exposure Windows data sets support these objectives and key purposes of the app:

- promote behaviour change by helping people manage their risk exposure by improving the accuracy of alerts;
- identify and inform people to help communities manage public health emergencies by contributing to knowledge about COVID-19 infection and risk of infection through the analysis of the Exposure Window data;
- support and inform users during isolation through this improved functionality and analysis.

The GAEN provides digital contact tracing to enable app users to support the wider response to the COVID-19 public health emergency.

The relevant design objectives are:

- helping the community (analytics)

The relevant purposes of the app as set out in the DPIA:

- COVID-19 symptom identification and monitoring
- alerting users if they have been in contact with someone who has tested positive for COVID-19 or been to a high-risk location or area
- responding to the public health emergency

The relevant primary purposes of the app are:

- to alert users when they have come into proximity with someone who has tested positive for COVID-19
- to support decision-making and advice to meet public health demands regarding the COVID-19 public health emergency
- to enable public health management and provide information to app users’, the public and those managing public health

This section sets out how the Exposure Window processes data and how it supports the objectives and purposes of the app.

We have updated Appendix 5 User Data Journeys with examples of the Exposure Window process.

How Exposure Windows Work (Processing of data)

The Exposure Window works as part of the Exposure Logging and Exposure Notification which is described in the section on digital contact tracing.

The key is the sharing of broadcast codes, or RPIs, with other app users which enables, through cryptocracy, for data but not identity to be shared between app users.

The Exposure Window, Exposure Logging and Exposure Notification process becomes relevant once an app user gets a COVID-19 test result.

Step 1. Updating Your App with your COVID-19 status

The app user receives their test result and updates their app

- For app users who begin their testing journey in the app, this occurs automatically
- For others, they will need to add their test result to the app

If the app user has tested positive for COVID-19 they are prompted to share their Diagnosis Keys.

For other app users, they will be prompted for relevant advice (for example, if they need to seek a further test or can end their self-isolation).

Step 2. Sharing your Diagnosis Keys with onset of symptoms data

- Choosing to share Diagnosis Keys allows other app users to be alerted if appropriate
- This will include the Diagnosis Keys for all the relevant days and the onset of symptoms data;
- The Diagnosis Keys are sent to the central system
- They are added to the reference list of Diagnosis Keys provided to all app users
    - This is updated approximately every 2-hours (allowing prompt but not instantaneous notification)

Step 3. Matching Diagnosis Keys and Broadcast Codes

Each app, technically within the GAEN functionality, reviews the Diagnosis Keys in the reference list;

If any broadcast codes held can be derived from a Diagnosis Key, then:

- the app user has been in touch with an index case (i.e. another app user with COVID-19)
- the app will calculate the risk of infection using the risk algorithm and the details held about the Exposure
- if the calculated risk, risk score, is above the risk threshold then the app will alert the app user and provide advice (for example, to self-isolate)

The data used for this calculation includes the Exposure Window and Scan Instance data sets.

The Exposure Window data set captures, for a 30-minute period.

- The date of the exposure (date)
- List of the Scan Instances within the Exposure Window (List of Scan Instances)
- The Risk Score version (Risk score version) for the Exposure Window to understand the basis of the calculation and which algorithm was used

This is used to check that the appropriate risk algorithm was used, and the calculated risk score

- Infectiousness of Index Case (Diagnosis Key) based on the date of the interaction between the users and the onset of symptoms data for the Index Case
- The Risk Score produced

Within each Exposure Window, the Scan Instances data sub-set captures:

- A minimum distance measure (minAttenuation) approximated via BLE signal strength
- The typical distance measure (Typicalattenuation)
- Duration (Timesincelastscan) the seconds elapsed since the previous Scan Instances

Neither the Exposure Window or Scan Instance data sets can or are attributed to any app user or to the two app users involved in the interaction by the NHS COVID-19 app and its supporting systems.

Step 4. Submitting the Exposure Window and Scan Instance data sets

Where an Exposure Window is generated it will be uploaded to the apps support systems, held on DHSC Secure Infrastructure; see section 'security of processing' for more information

The GAEN functionality determines when the Exposure Window are sent to the Product Environment, this process uses a number of privacy-preserving techniques to protect the identity of app users. These include:

- Within a 24-hour period randomising when the Exposure Windows are sent (preserving the privacy of app users by preventing any allocation of a time to an interaction between users)
- Ensuring that no identifiers are associated with either app user, including the Diagnosis Key
- Around 2.5 percent of Exposure Windows that result in a risk score above the current risk threshold are stored and captured. This sampling exercise supports the validation and monitoring of the app detailed above.
- Further privacy preservation techniques are undertaken once the Exposure Window data set and contents arrives at the product environment. These are detailed in section Digital Contact Tracing: Exposure Window and Appendix 5.
- The data is then passed to the app's analytical environment.

See Appendix 5 for User Data Journeys for an example of the data generated as part of app use and interactions with index cases.

Analytical Data Set

To ensure that the Exposure Window is functioning as expected a number of data items will be added to the analytical data set. This is part of ensuring that the service and function is working as expected. As part of evaluation of the service, the analytical data set will include a count of:

Total non-risky matches between Diagnosis Keys provided to the app and Broadcast codes held in the app. These are Exposure Windows that result in a risk score below the risk threshold set for that period;

Total risky matches. These are Exposure Windows that result in a risk score above the risk threshold and result in the app user being sent an alert.

Further Developments of the Exposure Window and Analysis

The Exposure Window data set offers further support to key purposes of the NHS COVID-19 app as well as determining the effectiveness of digital contact tracing in the current public health context. These developments will:

Capture Exposure Windows where both app users have updated their app with a positive COVID-19 test, with the index case having shared their Diagnosis Keys

- In addition to other purposes, this change helps understand if the app is breaking lines of transmission for app users and getting a sense of the scale of the impact

Relevant Data Sets

The Exposure Window data set contains the following data items:

Data Item	Description
Exposure Windows: object	Used by GAEN Mode 2 and based on data recorded in the GAEN, when a broadcast code is received by an app user. The data object created when an encounter with an index case happens.
Exposure Windows: date	The relevant date of the exposure window
Exposure Windows: List of Scan Instances	Part of the Exposure Window object, contains technical data regarding the scanning that happens when two devices are in proximity, each window will contain multiple Scan Instances - this provides an approximation of proximity and duration of encounters
Exposure Windows: Risk score version	Reference note on which risk score calculation method was used. Allowing us to check the relevant risk algorithm that was used.
Exposure Windows: Infectiousness of Index Case (i.e. the app user who shared their Diagnosis Key)	Sharing of the Diagnosis Key, includes the ability to share the relevant data to calculate the infectiousness for the Diagnosis Key to be worked out. This helps calculate the risk score.
Exposure Windows: Risk Score	The risk score calculation from the measurements and risk basis
Exposure Window: isConsideredRisky	Validates whether the Exposure Window was equal or above the risk threshold for the app at the time it was generated.

Additional data items

The following data items are associated with each exposure window in order to support the public health management purpose of the app.

Data Item	Specific Use to support Exposure Windows
Local Authority (Area)	Please Note: subject to the re-identification protections for areas See Analytics Data Table above, Used to support the public health analysis of the data to understand differences across areas
Postcode District (Area)	Please Note: subject to the re-identification protections for areas See Analytics Data Table above, Used to support the public health analysis of the data to understand differences across areas
Phone Model	Enables the analysis of the data provided to account for and monitor the variations in phone model
Operating System	Enables the analysis of the data provided to account for and monitor the variations in operating systems
App Version	Enables the analysis of the data provided to account for and monitor the differences in the app version
Type of Event	Notes the type of event to support the accurate flow of data

The Scan Instances data sub-set contains the following data items:

Data Item	Description
Scan Instances: min Attenuation	minimum attenuation of the signal received during the scan (in dB) – will approximate a minimum distance for the encounter
Scan Instances: Typical attenuation	typical attenuation of the signal received during the scan (in dB) - will approximate as an average distance for the encounter
Scan Instances: Time since last scan	Seconds elapsed since the previous scan, typically used as a weight - will be used to understand the duration of the encounter

For the full evaluation of the data sets and how they align with the apps purposes and the Privacy and Electronic Communication Regulations (PECR), see the data dictionary in Annex A.

Relevant Data Flow

The Exposure Window data sets will be sent to the Product Environment, which supports the NHS COVID-19 app. This will be undertaken using the existing Analytics API. Once received into the product environment, checks ensure the privacy of users (see the section on the removal of any IP addresses) and the data is provided into the App Analytical Environment.

There are no new data flows of this data beyond that which is set out in this DPIA.

Compliance with information law

As part of assessing any change to the app, a review is undertaken to ensure that the change is within the existing legal framework for the app and supports the existing purposes for the app. How the Exposure Window data set, and its use in analysis, supports the objectives and purposes of the app is set out above. The Exposure Window data set and its use for these purposes falls within the existing legal framework of the app, that is detailed in the section 'Digital Contact Tracing: Exposure Windows'.

Assessments of PECR (Digital contact tracing)

The data set is strictly necessary for the digital contact tracing and Public health response management function of the app, which is relevant to PECR, see the section PECR for updates on the data items used to support these functions.

Automated decision making and Article 22 (GDPR) requirements

See section on automated decision making above which outlines the app's position about Automated Decision Making. The introduction of GAEN Mode 2 changes parts of method of risk calculation and the risk algorithm used but does not change the existing policy or approach to the recommendation provided by the app.

It falls in line with the power of the Secretary of State outlined in the section above and that processing remains necessary for substantial public interest, within the conditions set out in paragraph 6 of Part 2 of Schedule 1 of the Data Protection Act 2018.

Necessity and proportionality

The collection of this additional data items within the central informatics system is deemed necessary and proportionate to support the key purposes of the app as well as permit the evaluation of the app's effectiveness in providing digital contact tracing and its impact upon public health.

The use of the Exposure Window data set alongside the Analytical Data Set provides the best modelling of the risk of infection and ensures that the recommendation for isolate are accurate and appropriate. The scientific team that supports the app can use the data collected to improve the understanding of the risk of infection, how different factors (such

as time, distance and infectiousness of the index case) interact to create this risk and to continue to improve the app's performance.

In addition, the data allows the app's performance and impact to be evaluated and enables the risk algorithm (the calculation of the risk of infectiousness), the risk score and the risk threshold (the score required to trigger a recommendation to isolate) to be scrutinized.

Given the protections in place to protect the privacy of users and effectively anonymise their identity, the use of this data is proportionate to the purpose set out for the app. The data set maintains the key conditions of the use of data and is necessary to deliver and evaluate the purposes for the app.

For more information on the risk algorithm, risk score and risk threshold see the section on the risk threshold.

Real-time high-risk area matches (alert)

The app will give users the ability to view the current risk level in the local authority they live in based on the postcode district and local authority entered during the registration process. It will also alert them to any changes in this and provide advice on what users should do next to get further information and guidance.

Risk levels and alerts will be sourced from the Local Authority Watchlist determined by the Secretary of State for Health and Care drawing on epidemiological advice from the CMO, NHS Test and Trace, Joint Biosecurity Centre (JBC) and Public Health England. It identifies Local Authorities of greatest concern across the country.

The watchlist is produced by first considering the lower tier local authorities with the highest incidence rate and its trend, combined with a range of other indicators including the test positivity rate, an assessment of the local response and plans, and the trend of other metrics such as healthcare activity and mortality. The classification decision is therefore a blended assessment drawing on professional judgement. There are further details regarding alerts for app users in Wales and for app users in England.

To determine local risk levels and generate alerts, the app will match the postcode district users enter on registering for the app to the local authority in which that district resides. The user will then confirm the local authority matched to the postcode district is correct.

There are 343 local authorities in England and 22 local authorities in Wales, so the risk of identifying specific individuals from assessments formed at this level is extremely low.

The user journey flow for this feature can be found in relevant annex – alert user journey

App feature	What data does the user enter to use this feature?	Where does the data go/ is the data stored?	Does the app do anything automatically with the users' data?	What data does the app receive?	Can the user opt out of this feature?	Level of risk to personal data
Alert	Their postcode district of residence (= first section of post code)	The app will send the risk score for each district to all phones	The app automatically rechecks the risk score for the stored postcode district to identify updates	The risk score for all areas	The user can avoid seeing the risk score for your area by deleting the app.	Low

The data flows relating to the Alert feature are summarised in the diagram below:

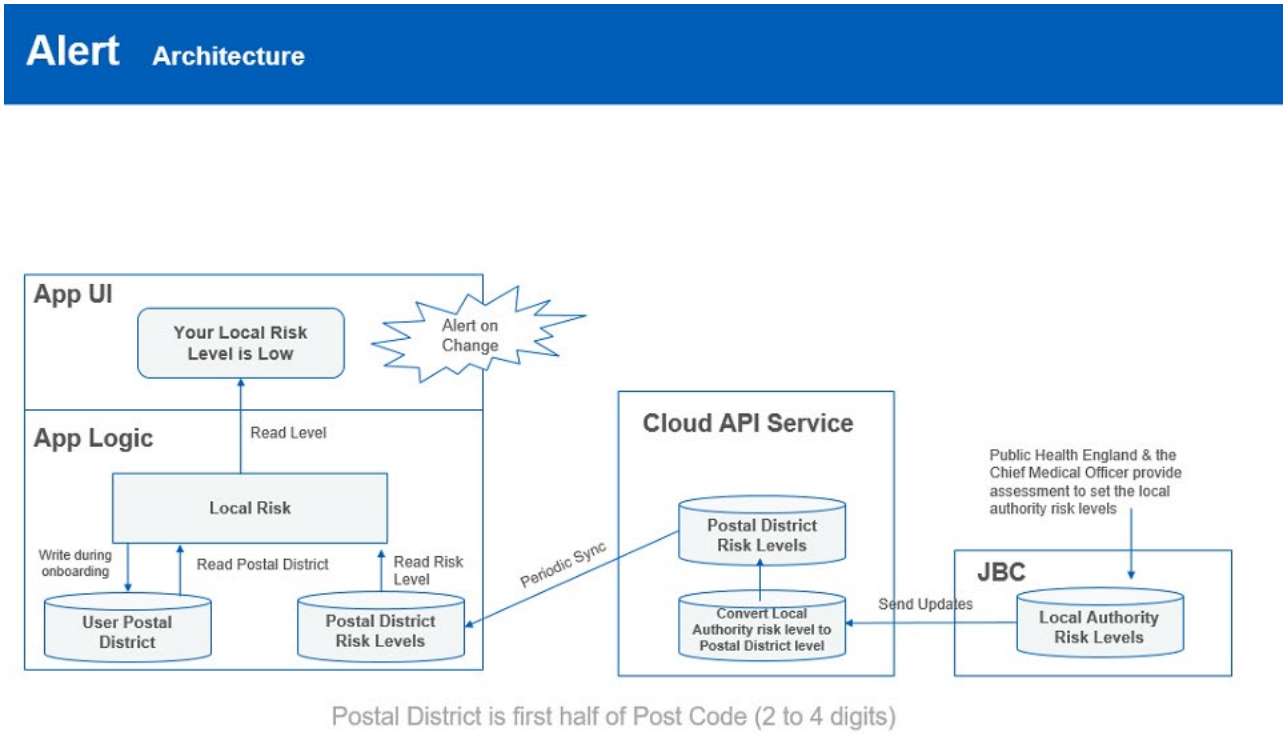


Diagram 1: alert architecture

Summary of requirements which led to this feature:

- there must be an alert if the user's postcode district is no longer risky
- the app must store the postcode district locally in an encrypted way to ensure of the user's privacy
- the current risk level for the user's postcode district must be shown on the home screen
- the app must check the user's stored postcode district against a provided cluster of known high-risk postcode districts in order to determine the current risk level for the user's postcode district
- the user must be notified if the risk level for the postcode district stored in the app changes
- the user must be able to enter the postcode district (first 2-4 characters of postcode) in the onboarding journey of the app. This step is mandatory

Digital check-in diary (venue check-in)

Users will be able to ‘check in’ to a venue via the app. The user must have the NHS COVID-19 App installed (they cannot use native, or other, QR apps for this feature).

Venues across a wide range of settings will be encouraged to support this capability, including workplaces, restaurants, pubs, leisure facilities and anywhere else where groups of people are likely to gather. If any of these venues are later confirmed as the source of a COVID-19 outbreak, users who visited them during a specified period time will receive an alert from the app advising them of this and what they should do next. Discussions are currently underway with PHE to agree the content and form of this advice.

The app will give users the ability to collate a ‘Digital Diary’ of locations they have been to over the last 21 days stored locally on their device. Users will create this via the QR code feature to ‘check-in’ to venues they visit and record the date and time they arrived. This includes the postcode of the venue to enable the specific venue to be identified. App users also have the ability to delete this data.

The app and its venue check-in and alert capability will align with the following high-level summary of the process for identifying, confirming and responding to local outbreaks:

- Health Protection teams (HPT) identify and plan an appropriate response to COVID-19 outbreaks in their region working with local authorities

- To do this they receive data from manual contact tracing, and local sources

- Health Protection Teams (HPTs) and Local Authorities investigate and follow up if required to form an assessment of whether it is an outbreak and what measures are needed to contain it

- HPTs record details of outbreaks in the dedicated web application (called HPZone)

- Once checked that an alert is appropriate for a venue by the administrative team, details of these outbreaks (QR code, date and time window) are entered into the app system. It will broadcast a message to each instance of the app that triggers an alert for any app users who had been to that venue during a specific timeframe and could therefore have been at risk of exposure

This process was updated to better support Health Protection Teams and reduce the administrative impact upon them. The data from the HPZone systems and used by Health Protection Teams are used to understand the nature of the public health emergency and learn about potential outbreaks or patterns. The use of this data falls outside of this scope of this DPIA. The process above, updated since the publication of the last DPIA does not result in any more data being processed by the app or the supporting services.

Details of where a user has checked-in to are recorded securely on the device and are not shared with the App backend system or database. Data from this service cannot, therefore, be used to either track movement over time or re-identify the user. This data can also be deleted by the user.

The user journey flow for this feature can be found in the relevant annex – check in user journey

App feature	What data does the user enter to use this feature?	Where does the data go/ is the data stored?	Does the app do anything automatically with the users' data?	What data does the app receive?	Can the user opt out of this feature?	Level of risk to personal data
Check-In	The user scans QR codes of venues visited.	The phone retains the QR codes visited and when they were visited for 21 days	No. The data of where the user has been stays on the phone. The user may choose to use it as an aide memoir when talking to a human contact tracer.	List of QR codes with date and time for impacted venues.	The user can simply not check in to any venues. User can delete all or individual venues from their phone.	Low

The data flows relating to the check-in feature are summarised in the diagram below:

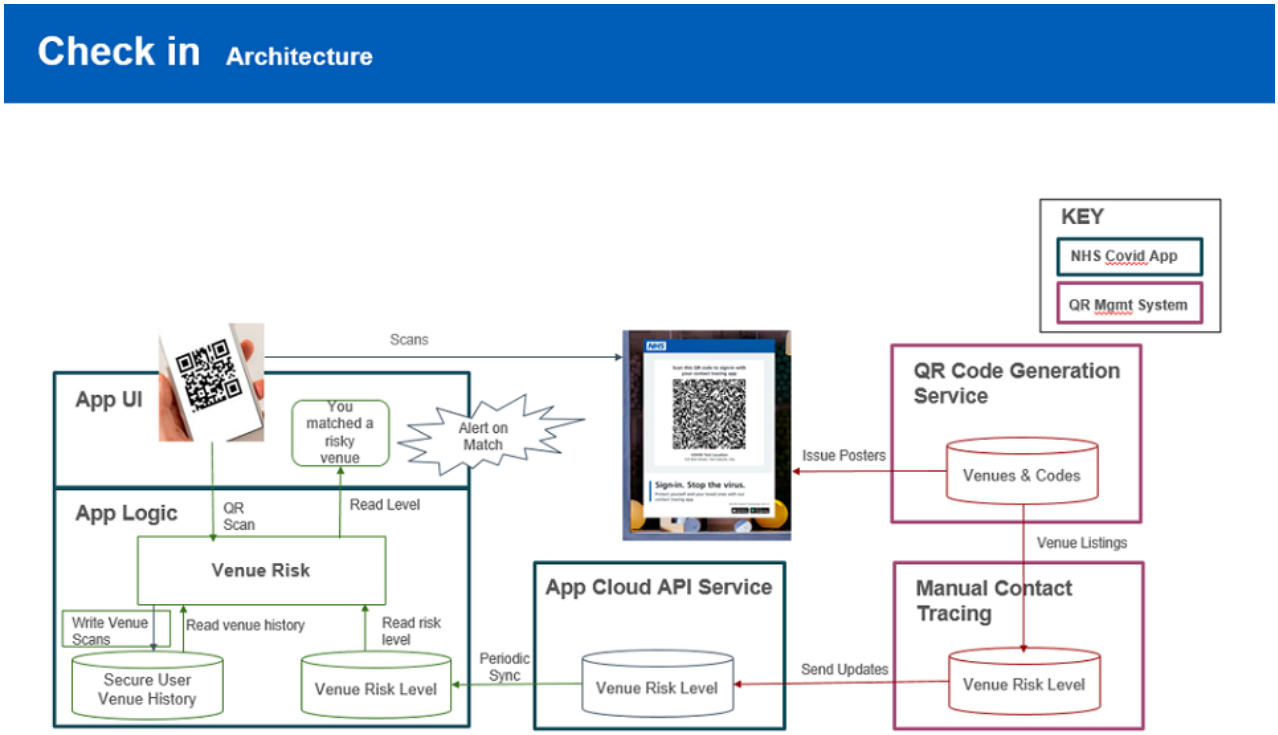


Diagram 2: venue check-in architecture

Summary of requirements which led to this feature:

- To be compliant with Apple's terms and conditions the scanned venues must be automatically and permanently deleted from the device after a maximum of 28 days.
- To be compliant with Apple's terms and conditions a readable list of captured venues must be readily visible to the user within the app.
- To be compliant with Apple's terms and conditions and for privacy reasons, all records of venue check-in activities are kept exclusively on the device.
- The venue name, ID and rounded check-in and check-out time must be shown in the venue history in "my data".
- The venue's postcode is included in the data displayed in "my data" on the app.
- The venue name and exact check-in time must be shown in the check-in confirmation.
- The app must store the following information: venue ID, venue name, venue postcode, timestamp of check-in (rounded down to last completed quarter), timestamp of check-out (rounded up to next completed quarter).

- It must be possible to suppress alerts about infected venues by a “circuit breaker” on the backend.
- There should be an option to cancel a check-in to cover the case that the user accidentally scans a wrong QR code (e.g. fake poster).
- The number of days the venue code is stored must be configurable.
- The app must provide automatic check-out options for visited venues. In v3/MVP check-out happens automatically at midnight or when there is a check-in to another venue.
- The user must be notified in case of a visited venue reporting high infection risk.
- The app must regularly check the stored user’s venue codes for high-risk venues.
- The app must securely store the scanned QR codes for a time configurable by the backend. The initial value is 21 days.
- The user must be asked to grant permission to use camera for QR-code scan.
- The app must enable QR code scanning from within the app and also when offline since connectivity might be limited at some venues.

Symptoms questionnaire (symptoms)

The app will allow the user to report the symptoms they are suffering with and the date of when they started. Based on which of the symptoms they have selected from a list, the user will receive an initial indication as to whether they may have coronavirus. If the user’s symptoms indicate they may have coronavirus, they will be asked to self-isolate and book a test.

The symptomatic questions are provided to the app team by the Chief Medical Officer (CMO) based on current epidemiological guidance. The questions and advice are captured in a version-controlled file on the DHSC secure computing infrastructure. As needed symptoms will be updated by the CMO. To capture the latest information, the questionnaire file is periodically synchronised from the back-end servers to make sure users are displayed the latest questions and advice.

For launch the current questionnaire includes the following symptoms: a high temperature (fever), a new continuous cough, a new loss or change to your sense of smell or taste, a runny nose, sneezing, feeling feverish, diarrhoea, nausea, vomiting, loss of appetite.

For those using the Wales version of the app there will be some differences visit the Test, Trace and Protect programme for details

The user journey flow for this feature can be found in the relevant annex – symptoms checker user journey

App Feature	What data does the user enter to use this feature?	Where does the data go/ is the data stored?	Does the app do anything automatically with the users' data?	What data does the app receive?	Can the user opt out of this feature?	Level of risk to personal data
Symptoms	User selects boxes relating to symptoms they have	Anonymised data on symptoms is retained for epidemiological purposes	No. The user actively chooses to submit their symptoms.	The app receives/holds the algorithm identifying if the symptoms checked according with COVID-19 risk	The user can avoid reporting any symptoms if they wish.	Low

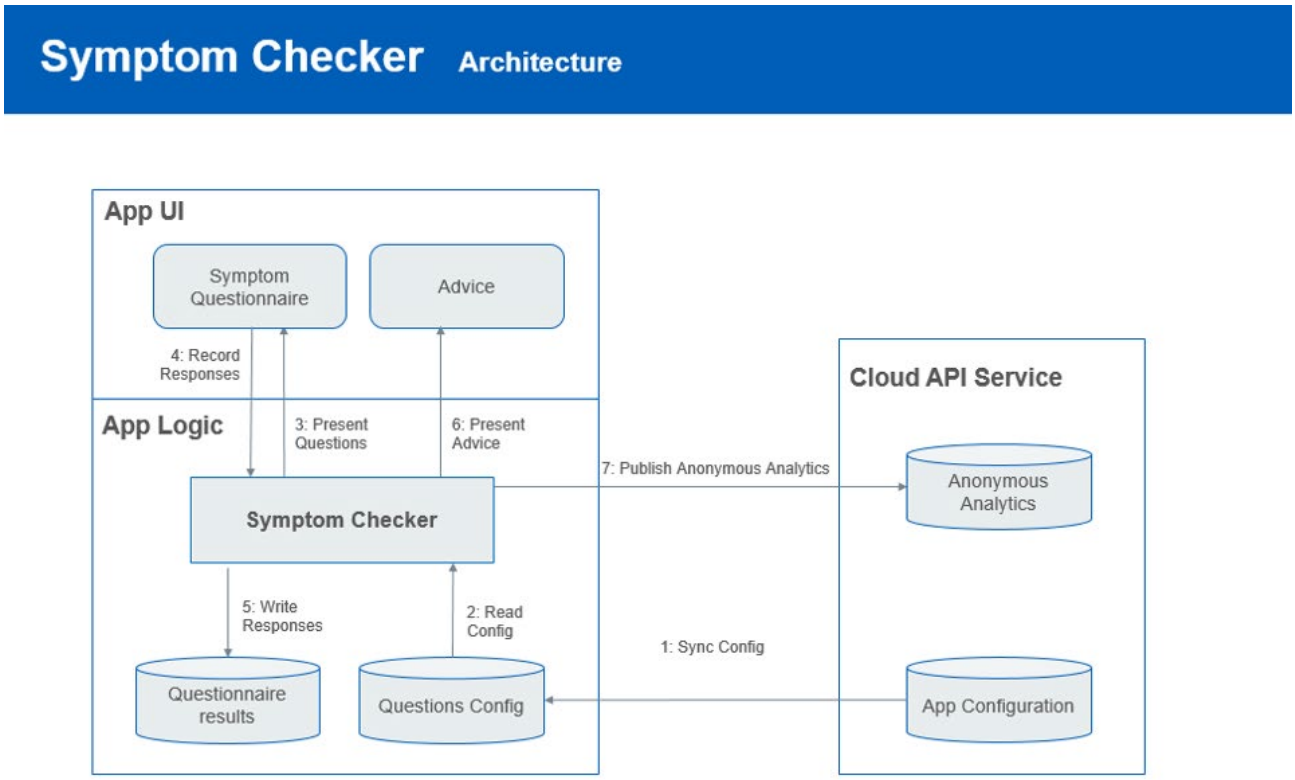


Diagram 3: symptom checker architecture

Summary of symptoms checker requirements which led to this feature:

- If an index case reports symptoms and is asked to isolate, the system should block the symptoms report for the isolation period. (This does not apply to contact cases).
- The algorithm evaluating the reported symptoms must be executed on the device in order to minimise the amount of data exchanged between the app and backend, and to ensure the backend is not considered a medical device.
- The user needs to give their permission every time any data reported on the symptoms report questionnaire is uploaded to the backend.
- The result of the questionnaire must be determined using a fixed algorithm.
- The symptoms report questionnaire must be configurable without the user having to update the app in order to quickly adapt to changes in policy.
- The default date for the symptoms onset in case users don't remember the date must be configurable as policy may change.
- The symptoms report questionnaire must contain a date for the onset of (all) symptoms in order to determine the remaining self-isolation period for the index case and to determine which contacts need to receive an exposure notification.

- The user must be able to quickly fill out the symptoms report questionnaire in order to increase the number of entries. It should therefore fit on a single page.

Coronavirus test (test)

A symptomatic app user will be invited to click a link from the iOS and Android applications to launch the testing service. Clicking the link within the app launches an external mobile browser and loads a page within the test registration journey with a unique app reference code (CTA token) and test reason (referralReason) passed as a query string parameter in the URL.

An example of this URL is below, where xxxx-xxxx is replaced by the unique CTA token and yyyyyyy is replaced with the test reason.

The new URL is:
https://self-referral.test-for-coronavirus.service.gov.uk/antigen?ctaToken=xxxx-xxxx&referralReason=yyyyyyy

Once the user has been taken to the testing website, they will follow exactly the same journey as users who visit the testing website via a different platform (e.g. computer browser), but the CTA token that was passed to the website will be associated with the test booking. The information captured during the standard test registration journey (such as name, date of birth, phone number, address etc.), will be stored in the relevant testing informatics technology system (NPEx), which is held separately to the app, along with the user's CTA token. The user will then take their test at a test centre or at home, and the test kit will be sent to a laboratory for processing. The CTA token is not sent to the test lab. The completed lab result (positive, negative or void), will then be sent to NPEx and re-associated with the app user's details.

If the test result received by NPEx is for a user who has a CTA token associated with their test record, then a three-field JSON file will be sent to the mobile application back end.

The fields are included in each file sent – the CTA token, the test result (positive, negative, void) and the hour range in which a test result was received. In addition, the token allows the type of test (for example, if it is a LFD or PCR test) to be determined.

The mobile application will poll the app back end to confirm whether a test result has been received. Once a result is received, it will notify the user whether they have a positive, negative or void test result. If the result is positive, the user will be prompted to share their Diagnosis Keys and enable the appropriate alerts of other app users.

The user journey flow for this feature can be found in annex 1 – risk score user journey. This is a visual file accessed by clicking a link from the page that also hosts this DPIA.

App feature	What data does the user enter to use this feature?	Where does the data go/ is the data stored?	Does the app do anything automatically with the users' data?	What data does the app receive?	Can the user opt out of this feature?	Level of risk to personal data
Test	The user clicks through to a website to order a test. The necessary data (e.g. address) is not entered into the app. The link that a user opens contains an 8-digit unique alpha-numeric code ("CTA Token") that the test system needs, in order to associate the user's app and test kit.	The test and trace programme retain the user's data long enough to associate the test taker with their result. Once the test result has been conveyed to the person, this data is deleted.	The 'early adopters' phase requires that the app reference code be passed to the test booking system. A user will not have the ability to edit this code during the booking process. An app user can still book a test via alternative channels if they do not wish for the app to be associated with a test kit.	If a user has started their test registration journey from the app, the mobile application will receive data that indicates whether a user has received a positive, negative or void test result. Other relevant information will be included such as the data of the test and the nature of the test.	If the user starts their test journey via the app, it will not be possible to opt out of the feature. However, a user can bypass this feature by visiting the test registration via a different channel.	Low

The data flows relating to the test feature are summarised in the diagram below:

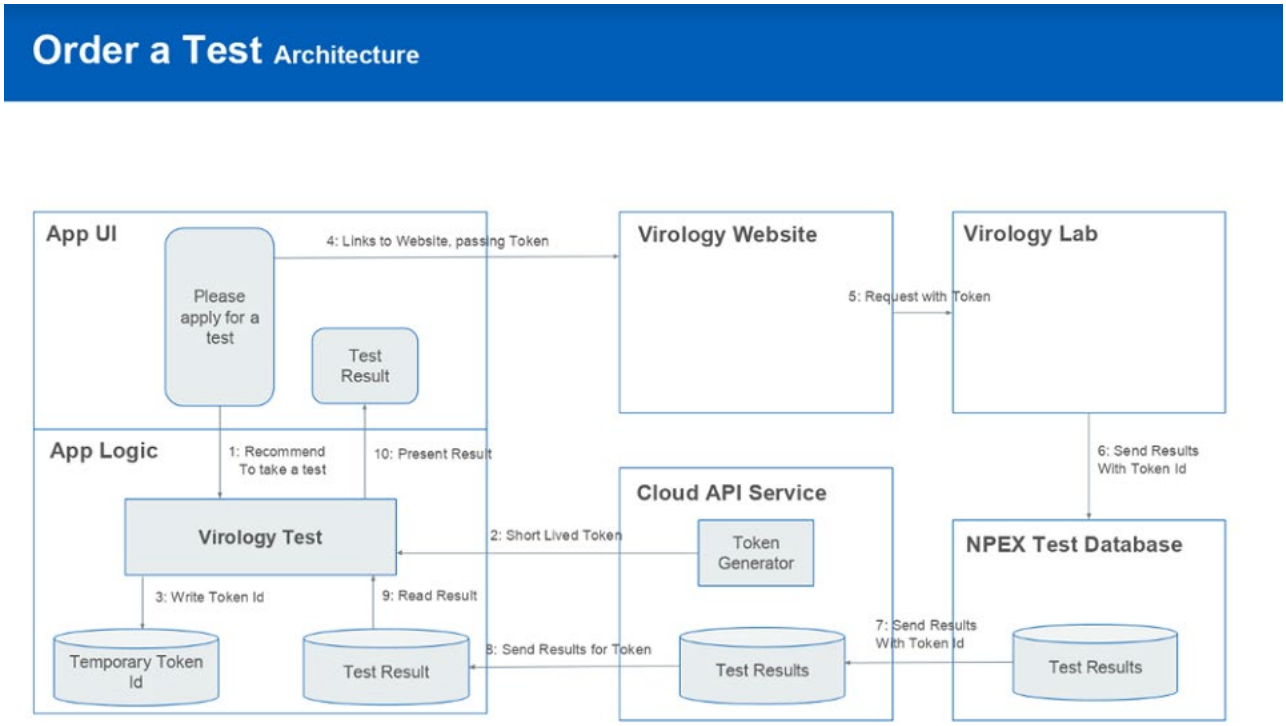


Diagram 4: ordering a test architecture

In addition to the overall data flow, the following is provided on how tokens will be generated, managed and secured. As per the diagram there are three tokens. All 3 are generated by the cloud service when an app user is recommended a virology test. The Lambda nodes refer to code that presents the respective APIs – listed above.

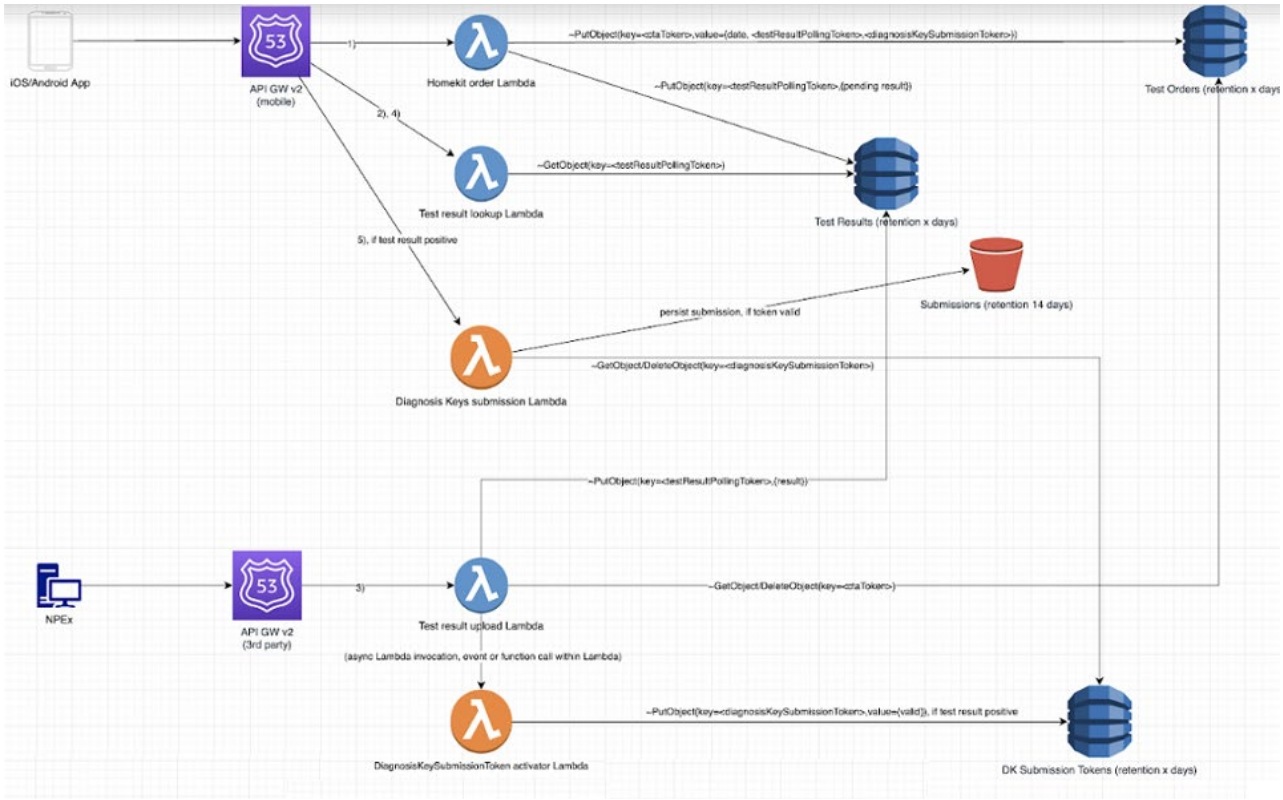


Diagram 5 showing how tokens will be generated, managed and secured

This includes the diagnosis key submission token, the test result polling token and the CTA token. Three tokens are employed as a security measure so that we do not use the same identifier in multiple locations.

The CTA token is the human readable random code that is displayed to a user and passed to the virology test system.

The test result polling token is the token used by the app to ask the DHSC secure computing infrastructure if the test result has been received yet.

The diagnosis key submission token is used by the app when a user is confirmed to be positive via test and gives permission to sharing their keys, so that the DHSC secure computing infrastructure can be sure the keys do relate to a confirmed positive case.

The Test Polling Token and the Diagnosis Submission Token are generated by the App Services hosted in AWS. They are unique, anonymous codes that are not derived from each other or any other keys, and are not composed of any other identifiers. A secure database within the App Services associates these three tokens (the third being the CTA token). The reason that three different tokens are used is for privacy reasons, so that the knowledge of the CTA token does not allow someone to poll for the results or submit diagnosis keys. All tokens are deleted once the test result has been delivered to the app.

The Test Polling Token, Diagnosis Submission Token and CTA Token are all created when the app asks for a CTA token when a user is recommended to take a test. They are retained in a secure database by the App Services only for as long as needed. All three are sent to the mobile app which stores the tokens in a Secure local store. The app uses the CTA token to pass to the Virology Testing website when recommending a test. The app uses the Test Polling Token when it is asking the App Services in AWS if a test result has been received. When the App Services receive a test result from Virology testing via NPEx, that will include a CTA Token. On receipt of the result the App Services will look up the Test Polling Token linked to the CTA Token and write the result in to a database together with the Test Polling Token. The CTA Token is then deleted. When the app next polls to see if a result is available, passing the Test Polling Token, the App Services will detect a match on Test Polling Token and return the result. The Test Polling Token is then deleted. The app user is then asked to submit their diagnosis keys, and when they do the keys are sent to the App Services together with the Diagnosis Submission Token. This Diagnosis Submission Token is required so the system can be sure that the submitted keys link to a genuine result. Once diagnosis keys are submitted the Diagnosis Submission Token is deleted.

The CTA tokens are unique, randomly generated codes of reasonable complexity, and it would be challenging for a malicious actor to guess a CTA token. If someone modifies the CTA token the most likely result is that the test result will be associated with an invalid CTA Token, which will be rejected when the unknown CTA Token is received from NPEx. In the highly unlikely event that an actor does manage to change the token to another valid CTA Token value that relates to a test currently underway, that would not allow them to access someone else's result, because they would not have the correct Test Polling Token. What it might mean is that the app user to which that CTA token relates would receive two test results.

Summary of test ordering requirements which led to this feature:

- The app generates a token whenever the user clicks on "book a test". This token temporarily links the user's test result to the app and thereby allows the result to be reported back to the app without entering personal details in the app.

- The user must be asked for permission before uploading the diagnosis keys stored on the user's phone. The request for permission is triggered after the user has seen the positive virology test result in the app. In order to avoid turning the app into IVD, it must not be the primary source for reporting the virology test result to the user.

- For v3/MVP the app must ensure automatic result retrieval and user notification of the virology test results for all test options connected to MPEX.

- The app must send a token to the virology testing website (in the background) when the user navigates to the website from the app.

- The app must allow the order of a test kit and will do this by providing a link to the virology testing homepage from within the app. In v3/MVP this is only provided to users who have reported symptoms in the app and are still in self-isolation.

The diagnosis key submission token is used by the app when a user is confirmed to be positive via test and permission to sharing their keys, so that the DHSC secure computing infrastructure can be sure the keys do relate to a confirmed positive case.

Self-isolation countdown (isolate)

The app will ask the user to self-isolate either because the user has reported symptoms indicative of coronavirus (the index case), or they have received an exposure notification (the contact case). Once asked to self-isolate, the user will have access to a self-isolation countdown which keeps a track of the time they need to spend self-isolating.

The data flows relating to the Isolation feature do not leave the phone. If users are experiencing COVID-19 symptoms, they can enter these into the app and they are used to provide advice about isolation. The isolation timing is configurable in a similar mechanism to the symptomatic questionnaire. The only data that is communicated to the back-end services in relation to the isolate feature is an analytics statistic to understand how many app users are currently self-isolating.

Where the user receives a positive test result, but no onset of symptoms date is available, the user will be prompted to enter one. This allows the app to provide guidance to the user that accounts for each testing and symptom pathway.

The user journey flow for this feature can be found in the relevant annex – isolate user journey

App Feature	What data does the user enter to use this feature?	Where does the data go/ is the data stored?	Does the app do anything automatically with the users' data?	What data does the app receive?	Can the user opt out of this feature?	Level of risk to personal data
Isolate	The user enters symptoms or a test result (see features above)	The app retains the date when a symptom entry was made so as to be able to offer a countdown until isolation ends.	If the user enters symptoms that accord with COVID-19 the app will automatically advise them to isolate. They may discuss this advice with NHS 111	This feature uses data entered into other features (see above)	Having entered positive symptoms, the isolate countdown will be automatically activated. The user could avoid this by deleting the app.	Low

Summary of self-isolation advice requirements which led to this feature

- If multiple test results come through in sequence for a given user, the first negative/positive test result will remove the user from being an index case/a contact case. The user will not be sent back to self-isolation based on later contradicting results.
- If multiple test results come through at the same time for a given user, only the most recent will be acted upon.
- The app must provide the user with information about the remaining self-isolation duration in days. In v3/MVP receiving new encounter notifications must not restart the self-isolation period if the user is already in self-isolation.
- The app must regularly check and compare the self-isolation period with the newest configurations based on policies.
- The app must alert the user if the remaining self-isolation period has changed or expired.
- The app must use a defined algorithm to determine the self-isolation duration depending on the type and date of the isolation trigger.
- Users can be a contact and index case at the same time. During that time the longer self-isolation period is displayed. The self-isolation countdown may therefore be adapted when a test result arrives.

- A contact case must not be released from self-isolation by a negative test.
- The durations of self-isolation for different cases must be configurable by the backend based on policy changes.
- The maximum duration for self-isolation must be configurable by the backend.
- The app must provide 3 triggers to stop self-isolation: Negative test result (index case only), isolation completed, isolation exceeded maximum duration.
- The app must provide 2 triggers for starting self-isolation: Reported Symptoms (index case), and Exposure Notification (contact case).

Functionality to pause the app exists whereby the Bluetooth-based contact detection can be temporarily disabled. No contacts, or exposure logs, will be made or recorded during the time that the pause is in effect. Users are provided with a clear visual indication on the home screen to indicate that contact detection is disabled. New functionality allows app users to set a timer when they pause the contact tracing functionality.

The ability to pause the app is provided to ensure that users who are in engaged in close proximity activities and have taken appropriate measures (such as a barber who is wearing a PPE face mask) can prevent erroneous exposure notifications.

Please note that guidance provided by the app can direct users to a website external to the app.

No interaction with the backend services is involved in this feature. Time idle during periods of pause is recorded by the app and submitted as part of the anonymous analytics data. This ensures that appropriate use of this feature can be assessed in aggregate.

These screens may slightly differ from those actually within the app:

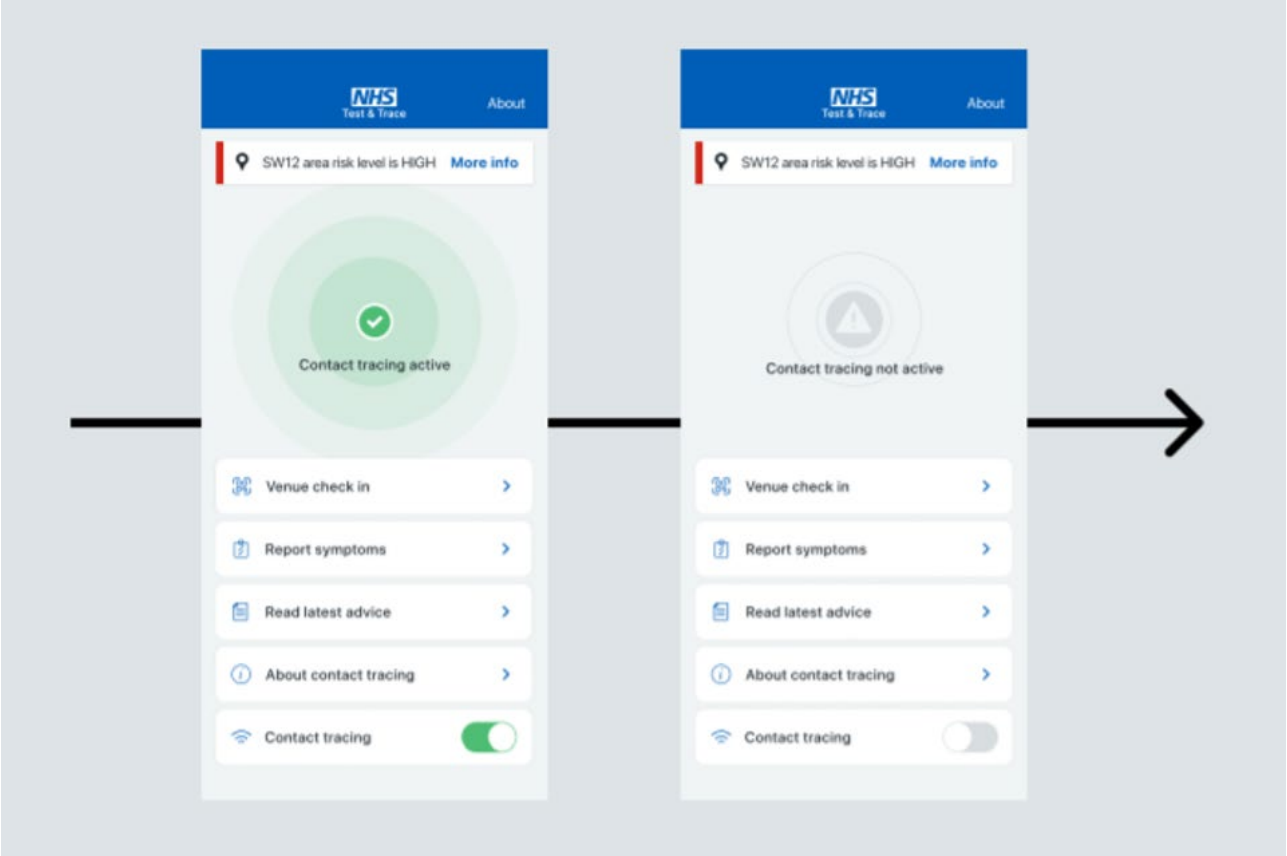


Diagram 6. Contact Tracing Screens

A visual indication on the home screen of the app indicates that contact detection is disabled.

Isolation Support Payment

The Isolation Support Payment will be known in England as the Test and Trace Support Payment (TTSP) and in Wales as the Self-Isolation Support Scheme (SISS). The Isolation Support Payment functionality allows an app user to start the process to apply for an isolation support payment from the app.

Applying for an isolation support payment places the app user under a legal obligation to self-isolation. This is regardless of whether they are confirmed as eligible for the payment. Information about eligibility is signposted to users from the app.

An app user can apply for isolation support payments when they are advised to isolate as a result of an exposure notification from the app. At the current time, this service from the app exists for England only. Welsh residents can access a site outside the app to apply, until system integration is built. See below for details of how and when the token and details to support the application are produced.

To use this service, England residents will need an NHS log in. If a user does not have one, they are able to create it as part of the process.

When the option is selected to seek financial support, this process will exit the user from the app and will take them to an external site known as the Gateway Portal. Exiting the app to complete the process of exploring eligibility for the isolation support payment, ensures the app does not capture any of the additional detail that is necessary for making an application for support. This preserves user anonymity in the app.

Isolation support payment also has another established process outside the app, which is triggered via manual contact tracing. Whether the process commences inside or outside the app, the individual is directed to the Contact Tracing and Advice Service (ITS) system. This system records information about people who have tested positive for COVID-19 and their contacts. Next they are directed to their Local Authority to execute payment.

A key point to note is that an app notification to isolate, based on exposure, is not legally enforceable. During the process of applying for an isolation support payment within the ITS system. However, the instruction to isolate becomes legally enforceable. To ensure this is clear, the Gateway Portal explains this process and will request permission from the user before they can proceed. Once permission is given in the Gateway Portal the legal duty to isolate is established regardless of whether or not the isolation support payment is paid.

An app user may receive a further exposure notification once their previous self-isolation period has completed, if they come into contact with another person who has tested positive, and therefore will need to isolate again. At this point, the app user is able to apply for a further isolation support payment. Provided the periods of self-isolation do not overlap, the process will commence again.

Once the app process to request financial support is started, a unique app reference code for an Isolation Payment Claim (IPC token) is generated to secure the interaction and data exchange between App, Cloud Services and the Gateway Portal. This portal allows the detail needed by CTAS (Encounter Date and Isolation End Date) to be gathered securely without impacting the privacy of app users.

The IPC token enables two factor authentication to reduce the risk of fraudulent tokens being created. Two factor authentication uses two systems and two different APIs for creating and verifying the token in order for the app user to be passed into CTAS' systems including the Integrated Trace Service (ITS).

- Factor 1: System "User/App" creates token with Isolation Payment Mobile API (Cloud Services) with Mobile-to-Cloud Services connection

- Factor 2: System "SIP Gateway" verifies this token with Isolation Payment Gateway API (Cloud Services) with Gateway-to-Cloud Services connection

The token allows the Cloud Services to associate data with the token, specifically the encounter date and isolation end date. Isolation end date is required to ensure the isolation period is still in effect. The user is encouraged to register for the isolation support payment as soon as possible to support the intended behaviour of isolating. It is important that the app isolation end date and the end date used by the CTA Service are identical, otherwise the app isolation period may differ from the legally enforceable isolation period.

The Gateway Portal will verify whether the user is from England or Wales. In Wales, although the IPC token is created, the process cannot progress until the Welsh integration with this solution is built. Therefore after a maximum of 14 days a token from a resident of Wales will be deleted. 14 days is also the maximum retention for an IPC token for an English app user (further details in the table below). Until integration for Wales is built, Welsh residents can access a site outside the app to apply.

App Feature	What data does the user enter to use this feature?	Where does the data go/ is the data stored?	Does the app do anything automatically with the users' data?	What data does the app receive?	Can the user opt out of this feature?	Level of risk to personal data
Isolation Support Payment	No data is entered by the user. They press a button to request financial support based on a message to isolate as a result of exposure (not symptoms).	The app system's Cloud Services creates an IPC token. Encounter date and Isolation End dates are associated with the token and stored in the app backend (cloud services). In the first step, only the token is transferred to the Gateway Portal. When the user is confirmed as residing in England, the gateway will pull the dates from the app backend. The token persists until the ITS application is started. At this point the token is deleted. It is expected this will occur within 24 hours, however is dependent on how quickly the user moves through the process. If they fall out of the process and do not reach the CTAS (via ITS) application stage the token will be deleted within 14 days. In Wales the token will be generated, however as it cannot be used until the Welsh integration is available.	Yes, the app sends Encounter Data and Isolation End Date after it has confirmed the user is in England and has received the IPC token from the Cloud Services.	The IPC token is returned to the app.	Yes. The user may not be eligible for this payment or may not follow through with the steps required to initiate the process in the Gateway Portal. In which case the token, which has been created, will be deleted within 14 days.	Low

App Feature	What data does the user enter to use this feature?	Where does the data go/ is the data stored?	Does the app do anything automatically with the users' data?	What data does the app receive?	Can the user opt out of this feature?	Level of risk to personal data
		It will be deleted within 14 days.				

The data flows relating to the isolation payment feature are summarised in the diagram below:

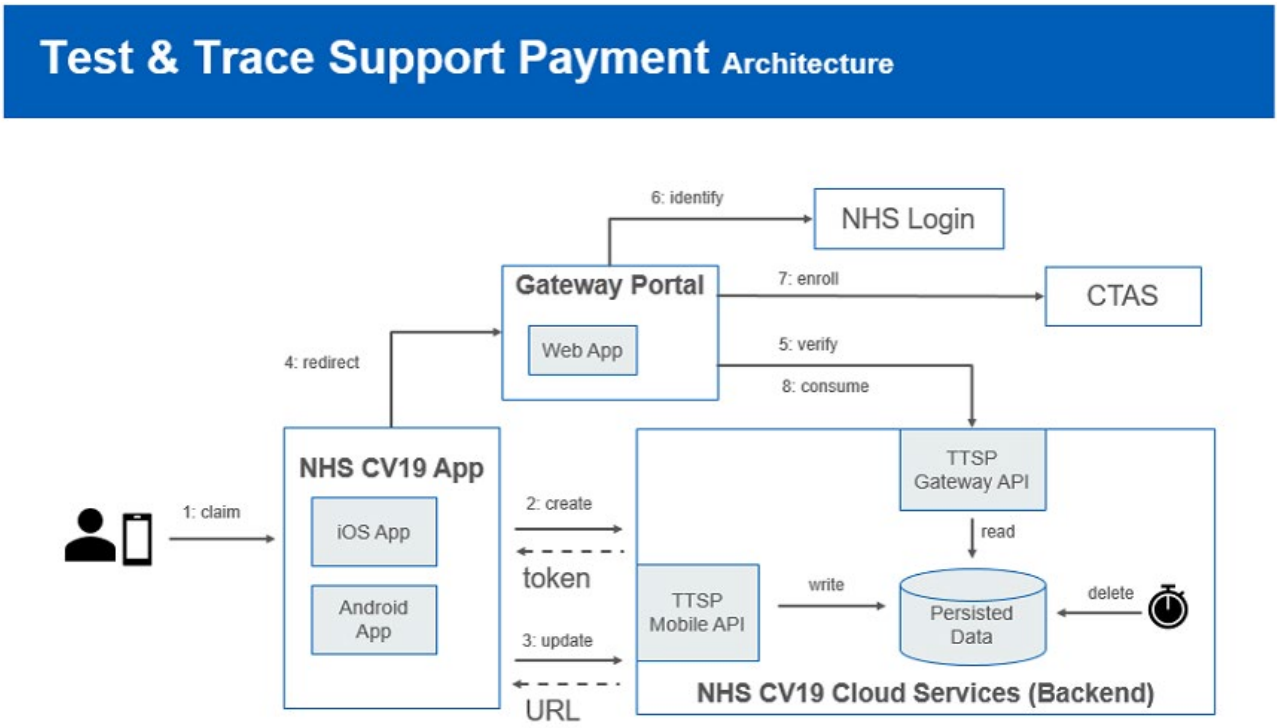


Diagram 7. showing isolation support payment architecture

The app recommends the user to self-isolate and displays a button to allow a user to enroll for financial support during this period.

- claim: The user pushes the button in the app to seek financial support.
- create: The app calls the Cloud Services (backend) which creates a new Isolation Payment Claim (IPC) token.
- update: The app transfers Encounter Date and Isolation End Date, and retrieves the Gateway URL (web page).
- redirect: The app redirects to the web page (Gateway Portal) which manages the enrolment process on the browser of the mobile device and in this process passes the IPC token.
- verify: The Gateway Portal uses the token to retrieve the Encounter Date and Isolation End Date.
- identify: The Gateway Portal verifies the user with an existing NHS system (NHS Login) which implements multi-factor authentication. If a user does not have an NHS login this process will allow them to create one in order to proceed.

- enroll: The Gateway Portal collects the necessary information to enroll the user to the service and sends the details to the CTA Services system (the ITS) for processing.

- consume: When the details have been sent to the CTA Service, the Gateway Portal will call the Cloud Services delete the token.

The Gateway Portal has an audit log where the tokens, timestamps and interactions with the other systems will be logged. No personal user information whatsoever will be logged or stored on the TTSP Gateway.

In order to validate that this service is work as required, the app will collect the following data items as part of the analytical data set. These data items cannot be attributed to a specific user. They enable the functions within the app to be checked and monitored against the isolation support payment portal. Analysis allows the counts of these functions to be monitored and as such acts as an early indication of faults or changes of use detected.

The data items to be collected as part of the analytical data set are detailed in the Data Dictionary, see Appendix 1.

Summary of isolation support payment requirements which led to this feature

This feature has been developed to ensure the app, which receives exposure notifications (an alert of a potential risk of infection), can seamlessly allow an app user to explore qualification for the isolation support payment, as they would if they had been instructed to isolate as a result of the manual contact tracing process.

Data protection impact assessment screening questions

Documenting which of the screening questions are applicable to your initiative will help to draw out the particular privacy considerations that will help formulate your risk register later in the template. This will also assist in ensuring that the Department's investment will be proportionate to the risks involved:

Ref	Question	Yes	No	Unsure	Comments
i	Is the information about individuals likely to raise privacy concerns or expectations e.g. health records or other information people would consider particularly private?	x	-	-	In the absence of proper controls, and transparency about how the App functions and how the data collected is used, the deployment of the App could give rise to privacy concerns.
ii	Will the initiative involve the collection of new information about individuals?	x	-	-	The Exposure Window and updated analytical data set involve additional data items collected about app users. However, they are within the existing legal framework, purposes and objectives of the app. They represent an improvement in the technology and analysis available for the app and its functions.
iii	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	x	-	-	Yes, the app can now support an user's application for support payments (a COVID-19 support payment, see https://www.gov.uk/test-and-trace-support-payment for England, and https://gov.wales/self-isolation-support-scheme, for wales). This the minimal amount of data to support the application process and ensure that the user is supported (for example, their self-isolation period is set consistently). However, the data items do not constitute personal data within the app or the apps systems.
iv	Will the initiative require you to contact individuals in ways which they may find intrusive?	-	x	-	-

Ref	Question	Yes	No	Unsure	Comments
v	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	x		-	Diagnosis Keys will be shared with app users in other jurisdictions. However, this is using the existing privacy and identity protections of the GAEN contract tracing system. This renders the Diagnosis Keys as anonymised to support interoperability.
vi	Does the initiative involve using new technology which might be perceived as being privacy intrusive e.g. biometrics or facial recognition?	x	-	-	Whilst the Bluetooth technology underpinning the proximity recording is not new technology, the use of the technology for this purpose in the context of a large-scale pandemic response is new.
vii	Will the initiative result in making decisions or taking action against individuals in ways which can have a significant impact on them?	-	x	-	No

Section 1: Background Information

Asset/Project Name

Organisation: Department of Health and Social Care

Assessment completed by: NHSX IG Policy Team and reviewed by the Test and Trace team

Name of IT BP: Barry McCormack/Tracy Strathie

DPO: Lee Cramp

Email: data_protection@dhsc.gov.uk

Section 2: Purposes

Project/Change Outline – Provide a description that provides an outside party with a good understanding of what the initiative is about.

The introduction at the start of this document provides a fuller description of the app.

The NHS COVID-19 App is a mobile phone application that is part of the NHS Test and Trace service. It is designed to reduce personal and public risk by providing support for:

- COVID-19 symptom identification and monitoring
- alerting users if they have been in contact with someone who has tested positive for COVID-19 or been to a high-risk location or area
- responding to the public health emergency

Aims/Objectives - Why is it being undertaken? What is the purpose of processing the personal information? What do you want to achieve?

The app aims to give citizens maximum freedom with minimum risk during a public health emergency by:

- driving safer behaviour by helping people manage their risk exposure
- identifying and alerting known and unknown contacts when transmission may have occurred
- enabling users to isolate and test to reduce transmission
- supporting and informing users during isolation

From the user's perspective, the app will help them take action to break the chains of transmission. Users are asked to:

- download the app and use it daily
- keep the app 'on' and carry their phone at all times
- follow instructions issued by the app
- 'pause' the app when appropriate
- enter symptoms and take a test quickly when required

To achieve the above the detailed primary of the app are as follows:

Primary purposes

The primary purposes of the app are:

- to facilitate self-symptom analysis for COVID-19
- to enable users to order tests and receiving test results
- to alert users when they have come into proximity with someone who has been tested positive for COVID-19
- to alert users when they have visited a venue that has subsequently found to have a significant number of confirmed COVID-19 cases leading to a risk of infection to app users
- to support decision-making and advice to meet public health demands regarding the COVID-19 public health emergency
- to enable public health management and provide information to app users', the public and those managing public health

These purposes are achieved by 2 key components:

- The app itself i.e. instances of the app downloaded and installed on users' mobile phones
- A DHSC secure computing infrastructure, hosted on Amazon Web Services (AWS) UK and Microsoft Azure Cloud Services (UK) supporting the app, which includes a database holding exposure notification diagnosis keys

These components function as follows:

The instance of the app installed on a user's phone

(a) Collects postcode district, allows the user to select the relevant Local Authority, and device type on installation and reports these to the DHSC secure computing infrastructure database

(b) Initiates the Google-Apple Exposure Notification API (GAEN) to record proximity encounters between users of the App on their respective devices, using Bluetooth technology, this includes the Exposure Window functionality which is part of GAEN Mode 2

(c) Gives users a risk score for their area and information relevant to their area, for example testing options or specific information such as variants of concern

(d) Provides a facility for users to check their symptoms and get advice on what to do

(e) Provides a facility of users to submit their Diagnosis Keys to the Cloud Services database should they be tested positive for COVID 19

(f) Receives Diagnosis Keys from the DHSC secure computing infrastructure database from users that have submitted them on positive diagnosis for COVID-19

(g) Interacts with the GAEN to establish whether an exposure event with an infected user has taken place and alerts the user should this be the case with advice on what to do

(h) Provides a facility for users to scan QR codes for venues they visit

(i) Obtains QR codes for venues that have reported infections, matches them to those visited and alerts them if a match with advice on what to do

(j) Provides a facility for users to request a one-time use token which they can use to order a test for COVID-19

(k) Receives the result of the test through the App from the Cloud Services database and reports this to the user (results can also be obtained through text/email to the user)

(l) Allow the app user to manually enter a test code with an associated result to update their and other user's status

(m) Reports an anonymous analytics data set to the DHSC secure computing infrastructure database.

(n) Supports the user if they choose to seek support payment as a consequence of a recommendation to self-isolation

The Local Authority is collected as part of the analytical data set and is subject to the same standards and controls to remove the risk of re-identification.

DHSC secure computing infrastructure

(a) Receives Diagnosis Keys submitted by users that have tested positive for COVID-19

(b) Distributes these keys to all users' apps

(c) Receives and distributes the QR codes for infected venues

(d) Issues a unique one-time use token which users can use to order a test for COVID-19

(e) Receives the results of tests and relevant details ordered from swab testing systems using the one-time use token

(f) Reports test results and relevant details back to the app on request using the token

(g) Collects analytics data on a regular basis, currently daily.

(h) Collects event analytics data on a regular basis, see section 'Securing data in transit'

See this document's appendices for the data dictionary, APIs presented by DHSC secure computing infrastructure and Operational Stages.

Interoperability via federated servers to DHSC secure computing infrastructure

(a) provide diagnosis keys to the federated servers from app users who have provided permission from England and Wales

(b) ensure the accuracy and completeness of the data provided through with supporting information to enable their use and ensure service management, for example, a count of the number of Diagnosis Keys submitted on each occasion

(c) download Diagnosis Keys from Federated Servers from other jurisdictions within the interoperability agreement, see the interoperability section for more detail

(d) ensure these diagnosis keys are made available in the appropriate format with the relevant test type to support digital contact tracing through the DHSC secure computer infrastructure and the only each partner to apply their testing and isolation policy

Performance and usage

The DHSC secure computing infrastructure database holds the anonymous analytics dataset specified in the Data Dictionary – see this document's introduction and appendices.

The separate App Analytical Environment is currently hosted in Microsoft Azure. Additional safeguards exist to support processing of anonymous analytics data transferred from the DHSC secure computing infrastructure database to this separate database.

The data protection impact assessment for the initial NHS COVID-19 app helped shape and inform this DPIA.

Section 3: The data involved

Information that identifies the individual and their personal characteristics

There must be justification for processing a particular dataset.

Area (postcode district and local authority)

Justification: Postcode district (the first digits up to the space) and local authority are needed to show users the COVID-19 risk level in their local area, and to collect data about the broad location of the disease to manage the public health emergency.

Medical/health/genetic information

Justification: Self-reported information indicating that a user has symptoms potentially of coronavirus (these reside temporarily on the local app before submission in anonymous form to DHSC secure computing infrastructure) is used to advise the user on whether their symptoms may be coronavirus. Test results received into the DHSC secure computing infrastructure database and local app inform public health planning as to the broad prevalence of coronavirus. Data indicating that a user has been in proximity with another user that has reported COVID-19 symptoms is used to inform users of their potential exposure.

The submission of diagnosis keys to the DHSC secure computing infrastructure indicates positive COVID-19 diagnosis – but is not considered personal data.

Unique identifying codes

Justification: Cryptographic keys (diagnosis keys/rolling proximity identifiers) with no link to user identity (direct identifiers) held by the controller are used to enable digital contact tracing.

Sensitive/special category of information

Information relating to the individual's physical or mental health condition

As set out above, the app ensures personal data is only stored on the phone and information that is held centrally does not identify the user.

Justification: Self-reported information indicating that a user has symptoms indicating that they may have coronavirus (these reside temporarily on the local App before submission in anonymous form to DHSC secure computing infrastructure). Test results received into the DHSC secure computing infrastructure database and local app. The submission of diagnosis keys to the DHSC secure computing infrastructure indicates positive COVID-19 diagnosis – but is not considered personal data.

Data supporting interoperability

Diagnosis keys are exchanged with the federated server. The keys are associated with a positive test result for COVID-19 and with their jurisdiction of origin. In this case England and Wales. For interoperability, diagnosis keys are treated as anonymous in GDPR terms.

Section 4: Overview of processing, necessity and proportionality

Why is the processing of personal data necessary?

The functionality of the app and nature of the data are explained in the introduction of this document.

Research and public health management

Users are asked to provide their postcode district – that is, the first portion (up to the space) of the users' home address postcode (e.g. SW1A) when they initially install the app. The app will not collect data about which postcode district a user might be in from time to time as they move around and nor will it link the person's identity to the postcode district they have entered. There is verification that the user has entered an actual postcode district (i.e. the app checks whether such a postcode district exists) but no checking that the user has entered the postcode district in which they live.

The postcode district and local authority data will primarily be used for alert notifications to users about changes in local risks, but may also be used for public health planning purposes, in conjunction with reported diagnoses and proximity information (for example, to help Local Government and NHS organisations to understand the spread of the disease

in their area), and may also be used for research purposes. Such research will not have impact on individuals and would address GDPR requirements in relation to research e.g. the safeguards set out in Article 89.

Section 5: the organisations involved and their roles

Are other organisations involved in processing personal data? If yes, please complete the table below.

Name	Please state whether they're a data controller (DC) or a data processor (DP)
Amazon Web Services	Processor (Hosting of Cloud Services)
The Health Informatics Services (THIS) hosted by Calderdale and Huddersfield NHS Foundation Trust (CHFT) utilising the NPEx	Processor (Provision of test code with result)

Has a data flow mapping exercise completed? See appendix 3

Does the project involve employing contractors external to the organisation? Yes

Data processors – Amazon Web Services: Cloud hosting services, hosting for DHSC secure computing infrastructure database

How is the information collected by this organisation? Electronic

Where will the information be stored? (including country location of data storage/back up) Amazon Web Services – cloud hosting servers located in EEA.

How will the information be kept up to date? Local instances of the App (user mobiles) interacting with the app; Communication of test results from National Pathology Exchange. AWS have no direct interaction with the data.

Which team(s) and roles have access to the information within this organisation? N/A – hosting only

What security measures are in place to protect this information from unauthorised use?

Security measures set out in the AWS GDPR Data Processing Addendum.

5) Security of Data Processing

5.1) AWS has implemented and will maintain the technical and organisational measures for the AWS Network as described in the AWS Security Standards and this section. In particular, AWS has implemented and will maintain the following technical and organisational measures:

(a) security of the AWS Network as set out in Section 1.1 of the AWS Security Standards;

(b) physical security of the facilities as set out in Section 1.2 of the AWS Security Standards;

(c) measures to control access rights for AWS employees and contractors in relation to the AWS Network as set out in Section 1.1 of the AWS Security Standards; and

(d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures implemented by AWS as described in Section 2 of the AWS Security Standards.

10) AWS Certifications and Audits

10) AWS ISO-Certification and SOC Reports. In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will make available the following documents and information:

(i) certificates issued in relation to the ISO 27001 certification, the ISO 27017 certification and the ISO 27018 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017 and ISO 27018); and

(ii) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls

AWS GDPR Data Processing Addendum 5 implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).

Is there a Data Sharing Agreement/protocol/data processing agreement in place? Yes – the AWS GDPR Data Processing Addendum

Data Processor – The Health Informatics Services (THIS) hosted by Calderdale and Huddersfield NHS Foundation Trust (CHFT) utilising the NPEx: processor (Provision of test code with test result)

How is the information collected by this organisation?

Data is provided through the testing process, with the data subject (the user undergoing test) informed of the process. They have a choice to use the app-generated test code or not. The test code and result are taken from the testing process and provided via NPEx to the App central system.

Where will the information be stored? (including country location of data storage/back up)

Calderdale and Huddersfield NHS Foundation Trust (CHFT) systems, based in the UK

How will the information be kept up to date?

Long standing systems and processes meeting Lab quality standards for accuracy and currency subject to UKAS oversight and ISO15189 compliance.

Which team(s) and roles have access to the information within this organisation?

Test Result Database and system (NPEx) support team.

What security measures are in place to protect this information from unauthorised use?

The system and service are subject to the standard expectations on an NHS organisation for processing personal data. This is measured through audit, testing and the Data Security and Protection Toolkit

Is there a Data Sharing Agreement/protocol/data processing agreement in place (as applicable)?

The NPEx service provided by THIS is subject to the standard contracts conditions of an NHS Foundation Trust supplemented by the requirements of the lab information systems.

Note on Apple and Google

Apple and Google are considered independent data controllers or controllers for the services which support the app. Any processing they undertake is distinct to processing of personal and other data by the app.

Section 6: assessment

Data protection principle: lawfulness, fairness and transparency

What is the legal basis for processing the information? (see appendix 3 & 4 for legal grounds for processing)

6(1)(e) "…exercise of official authority…"

Underpinned by section 2A of the NHS Act 2007 which provides the power that the Secretary of State relies on to authorise the design, implementation and operation of the App by DHSC\

For special categories:

9(2)(g) "…necessary for reasons of substantial public interest in the basis set out in [law]"

Underpinned by DPA 2018 – Schedules 1, Part 2, para 6 - Statutory and government purposes relating to public health and in particular the management of the COVID-19 public health emergency

9(2)(h) "…necessary for the management of health or social care systems and services…"

Underpinned by DPA 2018 – Schedule 1, Part 1, s. 2(2)(f) – Health or social care purposes

This condition applies because it is necessary to process the personal data for symptom checking and test management as this is an essential process in delivering care to App users.

9(2)(i) "…necessary for reasons of public interest in the area of public health…"

Underpinned by DPA 2018 – Schedule 1, Part 1, s. 3 – 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.

This condition applies because the objectives of the App include public health planning.

See the section on 'confidential patient information' and table above.

Is the processing of an individual's information likely to interfere with the 'right to privacy' under Article 8 of the Human Rights Act?

No. Although DHSC could invoke the exception in Article 8(2) "…where necessary in a democratic society…for the protection of health…" the decentralised approach built on the Apple/Google API achieves its objectives without the necessity to interfere with this right.

Robust privacy and identity protection of app users, alongside the voluntary use of the app, ensures that choice and the right to privacy is protected throughout the use of the app.

How and when are data subjects made aware of how their data will be used? E.g. Privacy statement

App users will receive a privacy notice via the App, that explains what information will be collected, how it will be used, the rights available to them, and sources of further information.

If you are relying on consent to process personal data, how will consent be obtained and recorded, what information will be provided to support the consent process?

Not applicable.

Do we inform individuals about the use of cookies and other tracking technologies?

Yes, information is provided to app users about the use of cookies

Do you receive information about individuals from third parties?

Yes – the DHSC secure computing infrastructure database will receive test results with temporary identifying token from the NPEx (National Pathology Exchange) system.

Data protection principle: purpose

Does the initiative involve the use of existing personal data for new purposes?

No. The data used to enable app users to claim support payments for isolation does not constitute personal data within the app and the app's systems.

Are potential new purposes likely to be identified as the scope of the initiative expands?

Yes – these would be related to the response to the COVID-19 emergency, efficacy of the App and services that users interact with.

Any change to processing of personal data would require revision to this DPIA.

As the Analytics data collected as a by-product of the operation of the App is anonymous, any new purposes for this data are unlikely to raise privacy concerns.

Are we consolidating and linking files and systems and if so how?

No

Are we changing the technology we use and if so, how are we mitigating the privacy affects?

No – this is an implementation built on the Google Apple API and noting changes to that system as it works. Any future changes would be subject to revision to this DPIA.

Data protection principle: automated decision making

Will the processing result in a decision being made about the data subject solely on the basis of automated processing (including profiling)?

See the section on automated decision making

If yes, is the decision necessary for entering into, or performance of, a contract between the data subject and a data controller? Or authorised by law based on the data subject's explicit consent?

No. See the relevant section.

Please describe the logic involved in any automated decision-making.

The design of the App's contact tracing function means that App users will be notified automatically if they come into sufficient contact with someone who has tested positive for coronavirus. The notification will advise them to self-isolate and may advise them to order a test. How the risk threshold is decided for issuing a notification is described in the section 'automated decision making'. It is integral to the design and operation of the contact tracing function that users be notified automatically, so that they can take appropriate steps to protect themselves, in a way that does not identify to anyone, including DHSC, or the person whose positive test result caused the notification to be issued. The App reminds users that they can phone NHS 111 if they have any questions or concerns about the notice to self-isolate in light of their personal circumstances (i.e. what the alert means, what they should need next, whether it is appropriate to obtain a test).

Data protection principle: adequacy

Is the data adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed?

Yes. Please refer to the section ‘nature of the data’.

How have you ensured that only the minimum data is used to meet the purpose of processing? e.g. each data item is justified and periodically reviewed?

All persistent personal data is held on the phone and is not accessible to the controller. With the exception of test results with their associated tokens (which are transient and short-lived) the data held on the DHSC secure computing infrastructure backend is anonymous.

How many individuals are processed through this system in a given time period?

The use of the app is voluntary. It will be effective at any level of uptake, but most effective if more people download and use it. We are expecting mass download and use of the app. If 80% of adult smartphone users use the app, it would represent around 56% of the population or around 37 million people

Data protection principle: accurate and up to date

How are personal data checked for accuracy?

Diagnosis Keys are generated by the GAEN and are not under our control. We rely on the GAEN to generate unique keys that are not repeated for each instance of the installed app. We also rely on the GAEN to generate Rolling Proximity Identifiers that are unique to an instance of the installed app. We also rely on the GAEN to re-generate the correct set of RPIs from diagnosis keys distributed by the DHSC secure computing infrastructure.

We are reliant on the user’s self-symptom analysis, but symptom checker questions have been carefully designed with professional oversight in line with overarching public health advice relating to COVID-19. We are reliant on the user to submit their postcode district but can check that it is a valid postcode district code. There is no verification as to whether the postcode district the user enters is the one in which they reside.

The anonymous Analytics dataset (and risk action etc.) are generated and submitted automatically by the App.

What action would be taken to correct inaccurate personal data?

Current implementation of postcode district validation uses the following:

Min length 2

Max length 4

Matches the regex ^[A-Z]{1,2}[0-9R][0-9A-Z]?

The user can delete and re-enter the postcode district if they have entered one in error (subject to the same validation outlined above).

How frequently is the personal data updated or what would trigger the information being updated?

Data on the users' phones is updated as they come into proximity with other users, so the frequency depends on this.

The DHSC secure computing infrastructure database is updated once (per infection) when the user submits their Diagnosis Keys. It is also updated when test results are received – so once per test request.

Is the quality of the information good enough for the proposed purposes?

Yes

Are the sources of the personal data recorded?

No. It is a privacy feature of the design of the App that this information is not necessary.

Data protection principle: retention

What are the retention periods for the personal information

See section 'retention of data from the app'

What is the justification for holding the information for this length of time?

See section 'retention of data from the app'

How will the retention schedule be managed and enforced?

See section 'retention of data from the app'

How often is this retention period reviewed?

At least every 6 months

Are there any exceptional circumstances for retaining certain data for longer than the normal period?

There are none anticipated at present however in the context of a national emergency this is a possibility.

How will information be fully anonymised, archived or destroyed after it is no longer necessary?

The diagnosis keys and analytics data held on the DHSC secure computing infrastructure database are anonymous when collected, refer to Appendix 5 for further detail.

The diagnosis keys are retained for a maximum of 28 days (14 days on the phone and 14 days on the DHSC secure computing infrastructure database). They are permanently deleted from the phone after 14 days, and from the DHSC secure computing infrastructure after 14 days from submission.

Test results and associated tokens are transient and short-lived.

Data protection principle: rights of the individual

How will you action requests from individuals (or someone acting on their behalf) for access to their personal information?

Subject access requests will be facilitated by a feature of the app to present all information held in the app on the phone. No data will be retrieved from the DHSC secure computing infrastructure database as there is no way to link the information held in the DHSC secure computer infrastructure to individual users.

There is a feature planned for a follow up release that allows a user to view all captured data on the app. Given that this data never leaves the app that is the only place they will be able to view it.

How would you locate all personal data relevant to an individual?

Personal data that can be located is on the phone

What is the procedure for this system to responding to data subject's request to be forgotten – Article 17

Users may uninstall the app from their phone at any time which will cause deletion of all the app data from the device. Although this will not cascade to the DHSC secure computing infrastructure database the diagnosis keys are deleted after 14 days automatically.

Article 16 – Right to rectification

Not available – controller does not have access to the personal data on the phone. If a user disagrees with a test result, they will need to contact the test provider.

Article 18 – Right to restriction of processing

Not available – controller does not have access to personal data on the phone.

Article 19 – Notification obligation regarding rectification or erasure of personal data or restriction of processing

Not available – controller does not have access to personal data on the phone.

Article 20 – Right to data portability

This right is not available because the processing is not based on consent pursuant to Article 6(1)(a) or Article 9(2)(a); or on a contract pursuant to Art. 6(1)(b).

Article 21 – Right to object

Available by uninstalling App. The user also has the choice not to use Venue-Check in functionality as well as the ability to delete both all or individual Venues

Article 22 – Automated individual decision-making including profiling

See section 'automated decision making'

Data protection principle: appropriate technical and organisational measures

What procedures are in place to ensure that all staff with access to the information have adequate IG/Data Protection training?

Both DHSC (the controller) and NHS England and NHS Improvement have well established mandatory IG training that must be accessed annually by all staff. This also applies to NHS Test and Trace.

How will the information be provided, collated and used by these staff?

DHSC – internal procedures

NHS England and NHS Improvement – online training provided and monitored via the Electronic Staff Record.

What are the access restrictions and permissions in place, including a JML process?

See section 'security of processing'

What are the security measures in place for this data?

Data are held on the user's device.

See section 'security of processing'

Data protection principle: transfers both internal and external including outside of the EEA

Will an individual's personal information be disclosed internally/externally in identifiable form and if so to who, how and why?

No.

Will personal data be transferred to a country outside of the European Economic Area? If yes, what arrangements will be in place to safeguard the personal data?

There are no expectations that personal data will be transferred outside of the UK or EEA.

Consultation

Identify both internal and external stakeholders

DHSC – the controller

NHS Test and Trace – part of DHSC, with overall responsibility for delivering the Test and Trace programme

NHSX – comprising DHSC, NHS England and NHS Improvement (TDA and Monitor).

The legal entities comprising NHS England and NHS Improvement provide resources/staff for DHSC through NHSX.

The Welsh Government and its Test Trace Protect programme is a stakeholder in so far as they have decided to make use of the app.

We have a stakeholder engagement plan which we are using to reach out to groups in the health sector, social care, patient representatives, communities, charities, business and academia to inform the development of the app. We are in dialogue with privacy groups and are engaged with the National Data Guardian, Information Commissioner's Office, Understanding Patient Data and the Centre for Data Ethics and Innovation.

Guidance used

Details of any link to any wider initiative or list any national guidance applicable to this initiative.

This initiative accompanies analytical work to support the COVID-19 emergency generally. The app's data storage is under the remit of the Test and Trace programme. However, no linkage of data between the data sources is possible.

Is the provision of personal data obligatory or voluntary?

The provision of diagnosis keys to the DHSC secure computing infrastructure database is a voluntary action for app users, requiring a positive action.

If obligatory, why/how is that the case?

Use of the app is voluntary and users who have downloaded it can delete it at any time.

No obligation to use symptom checker.

What are the possible consequences for a data subject if there is a failure to provide the requested personal data?

If a user does not upload diagnosis keys then opportunities may be missed to carry out proximity alerting for that user (and the other users with whom they had proximity encounters).

Outcomes

What will be the effects of the processing (i.e. what actions/decisions will result from the processing)?

Users will be (i) notified about proximity encounters that mean they may have contracted COVID-19, and given advice on the steps to take; and (ii) will have the opportunity to self-diagnose on the basis of a symptom checker (both apply if the user displays symptoms); and (iii) be given the opportunity to request a test for COVID-19; and (iv) be notified when they have visited a venue where cases have been reported

Common law duty of confidentiality

Are any of the data subject to a duty of confidentiality (e.g. clinical records, OH details, payroll information)? If so, please specify them.

Yes. Test code and results – held temporarily in the Cloud Services database.

(Diagnosis keys submitted to the DHSC secure computing infrastructure database indicate positive COVID-19 diagnosis associated with a set of derived rolling proximity identifiers. Neither diagnosis keys nor RPIs are considered personal data.)

Where it is planned to use or disclose such data, what are the grounds for doing so?

To enable a test result to be passed back to the user's phone, which will allow them to see it and be asked whether they are willing to release their Diagnosis Keys to the cloud so that the App's contact tracing function can be initiated. The Health Service (Control of Patient Information) Regulations 2002 set aside the CLDC for this purpose. Test results are used by the broader Test and Trace programme to support planning purposes in response to the COVID-19 public health emergency.

If the processing is of data concerning health or social care, is it for a purpose other than direct care?

Public Health Management

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

Does the processing engage the Privacy and Electronic Communications Regulations 2003 (as amended) ('PECR')? If so, how are the requirements of the regulations met?

See relevant section

Section 7: Risk register

The following risk register replaces the existing

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
R001	Transferring of data outside of the EEA without proper controls	Risk to individuals arising from inadequate controls to protect privacy in non-adequate country.	Non-compliance: No adequacy arrangement results in serious non-compliance with the data protection legislation. This faces regulatory action and exposes the vulnerability of an organisation	If consequentl y there is any loss of personal data to non-trusted sources this is a further breach and risks privacy re onward sharing of personal data; reputational damage; loss of trust	All data collected by the app and potentially accessible by any data processors is not directly identifiable (pseudonymi sed in GDPR) terms. ; Contracts and Data Processing Agreements are based on	Reduced (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
			as it is a breach.	by data subjects.	Government Cloud Framework and prevent processing outside of the EU only with permission and adequate controls (-, see GCloud framework); Ongoing contract oversight of any data processors ; Authorisation of User Access process ; Access						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Control and Audit Log of user access across environments ; Framework for onboarding/offboarding suppliers in line with NHS/DHSC requirements ; Nature of the analytical data set collected from app users ;						
R002a	Misuse of information	Loss of personal	Non-compliance	Vulnerability of	Limited and controlled	Reduced (Likelihood)	Sign off on Risk - Senior	06-Apr-21	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	by those with access within dedicated App Data Environments (Product and App Analytical Environments)	data to non-trusted sources; privacy risk due unauthorised sharing of personal data.	with data protection legislation.	organisation to data breach and possible regulatory action; reputational damage; loss of trust by app users	access to data environments (product) and systems that support the app , Staff contracts (both direct and if employed as data processors) ; Data Processing Agreements based on GCloud framework ; Data does not reveal app users identity ;		Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Ongoing contract oversight of any data processors ; Authorisation of User Access process ; Access Control and Audit Log of user access across environments ; Framework for onboarding/offboarding suppliers in line with NHS/DHSC						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					requirements;						
R002b	Misuse of information by those with access within dedicated App Data Environments (NHS Test and Trace Data Analytical Platforms)	Loss of personal data to non-trusted sources; privacy risk due unauthorised sharing of personal data.	Non-compliance with data protection legislation.	Vulnerability of organisation to data breach and possible regulatory action; reputational damage; loss of trust by app users	See DPIA for NHS Test and Trace Data Analytical Platforms (TTDAP) for controls within those environments; Data is analysed and processed prior to providing the data to NHS TTDAPs; Data is not user row level and is	Transferred (NHS TTDAP)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	06-Apr-21	1	3	Amber/Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					subject to additional controls to obstruct reidentification;						
R003	Inadequate data processing agreements with data processors.	Risk to individuals arising from inadequate controls to protect privacy.	Non-compliance with Article 28 requirements.	Vulnerability of organisation to data breach and possible regulatory action; reputational damage; loss of trust by data subjects.	Data sets associated with the app do not make app users directly or indirectly identifiable ; Limited, controlled and audited access to data stores and services ; Contracts in place with	Reduced (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	2	3	Amber/Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					suppliers including Data Processing Agreement (for example, covering data breaches) based on GCloud framework ; Ongoing contract oversight of any data processors ; Authorisation of User Access process ; Access Control and Audit Log of						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					user access across environments ; Framework for onboarding/offboarding suppliers in line with NHS/DHSC requirements ;						
R004	Lack of technical or organisational measures implemented to ensure appropriate security of the personal	Risk to individuals arising from inadequate technical or organisational controls to protect the data. Data	Non-compliance with the data protection legislation – in particular Article 32.	Vulnerability of organisation to data breach and possible regulatory action; reputational	Data held by the app product, backup or analytical is not likely to constitute personal data as	Reduced (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme	18-Sep-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	data	breach due to technical weakness (e.g. cyber-attack); access by unauthorised people.		damage; loss of trust by data subjects.	defined by GDPR ; Hosting arrangements are within standard NHS governance structures, subject to routine review and backed by contracts/oversight at least equivalent to GCloud ; Oversight and scrutiny by the National Cyber Security		Sign off for DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Centre [NCSC] ; PEN Testing undertaken on environment (-, PEN test report); Action plan and response to PEN test recommendations						
R005a	Personal data not being encrypted in transit	Risk to individuals arising from inadequate technical controls to protect the data. data	Non-compliance with the data protection legislation – in particular Article 32.	Vulnerability of organisation to data breach and possible regulatory action;	The data transmitted to the app, and between environments does not constitute personal	Reduce (Impact)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace	18-Sep-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
		breach due to technical weakness (e.g. cyber-attack); access by unauthorised people.		reputational damage; loss of trust by data subjects.	data or has protections sufficient to reduce or eliminate identifiability ; Data flows to the app from the environment are undertaken through secure methods ; Oversight by NSCS ; PEN test ; routine PEN testing PEN test and plan to implement recommendations ;		programme Sign off for DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
R005b	Personal data not being encrypted at rest	Risk to individuals arising from inadequate technical controls to protect the data. Data breach due to technical weakness (e.g. cyber-attack); access by unauthorised people.	Non-compliance with the data protection legislation – in particular Article 32.	Vulnerability of organisation to data breach and possible regulatory action; reputational damage; loss of trust by data subjects.	The data held does not constitute personal data or has protections sufficient to reduce identifiability ; Data is held on Amazon Web Services solutions, including S3, which is subject to security protections and encryption; The	Reduce (Impact)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	21-Apr-21	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Analytical environment is hosted on Azure services and is subject to similar controls ; PEN testing of environments ; Oversight by the NCSC ; routine PEN testing PEN test and plan to implement recommendations ;						
R006	Lack of testing which would	Risk to individuals arising from	Non-compliance with the data	Vulnerability of organisation	Limited identifiability of app users	Reduce (Impact)	Sign off on Risk - Senior Information	18-Sep-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	assess and improve the effectiveness of such technical and organisational measures	inadequate technical controls to protect the data. data breach due to technical weakness (e.g. cyber-attack); access by unauthorised people.	protection legislation – in particular Article 32.	to data breach and possible regulatory action; reputational damage; loss of trust by data subjects.	data rendering unlikely to be considered personal data (within the context of the app) ; Testing undertaken by contractor (Zuhlke) to ensure functionality and systems are tested ; Findings from Early Adopters programme (noting that this will involve live		Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					user data and needs to be managed appropriately) to test functions, scale and support services ; PEN test, recommendations and actions taken as a consequence						
R007	Inadequate or misleading transparency information	App Users are not appropriately informed about the controller, purposes for	Non-compliance with DP legislation in particular Articles 12 and 13;	Vulnerability of organisation to regulatory action.	Data and Privacy page in the app (as part of entry into system) ; Privacy	Reduce (Impact)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and	28-Nov-20	1	4	Amber

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
		processing, legal basis and other requirements of Articles 12 and 13.	reputational damage.		Notice for the app ; Communication campaign for public about app ; Outreach to community groups ; User Research (comms and app) Publishing DPIA ; Privacy Notice (Young Persons); Privacy Information (Easy Read); Learning		Trace programme Sign off for DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					from outreach programme; Publication of anonymisation, user data journey's and scenarios; Ongoing review of Privacy information						
R008	Misuse (by app user or those with access to the phone) of token issued by App for test requests and	If reference code obtained and used by another individual they could order a test pretending to	Non-compliance with statutory obligations and Data Protection legislation, in particular	Reputational risk. Failure to fulfil obligations towards app users.	Note: Mitigation relies on the action of the app use and those with access to their phone	Accepted	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme	18-Sep-20	3	1	Amber/Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	results management	be them.	accuracy				Sign off for DPIA - Data Protection Officer				
R009	Malicious access to Cloud Services database by cyber attack Extraction and re-identification of Cloud Services database data by combination with other data	Risk to individuals arising from inadequate technical controls to protect the data. Data breach due to technical weakness (e.g. cyber-attack); access by unauthorised people.	Non-compliance with the data protection legislation – in particular Article 32. Notifiable security breach. Breach of confidentiality. Reputational damage. Undermining purpose of app.	Reputational damage. Undermining purpose of app.	Data does not reveal app users' identity ; Technical protections in place ; Oversight by NCSC ; PEN Testing ; routine PEN testing PEN test and implemented recommendations ; Threat model of malicious	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	1	5	Amber

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					access to cloud services ; Summary of cyber risks, ongoing monitoring and reporting to senior Cyber Information Security governance ; Security Risk Mitigation Plan and ongoing work ;						
R010a	Identification of infected individual due to minimal	Identity of infected person implicitly revealed	Use of the App may be considered to breach confidentialit	Reputational damage. Undermining purpose of app.	Broader COVID-19 Public Health Emergency	Accepted	Sign off on Risk - Senior Information Risk Owner and Chief	18-Sep-20	3	3	Amber

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	contact - e.g. isolated person with carer who is only contact		y by implication.		context and contact tracing ; Contents of the Privacy Notice addressing point		Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer				
R010b	There is a risk for app users with limited social interactions that they might be identifiable or be able to identify other app users due to these limited social interactions	Reidentification (impact on privacy and anonymity)	Undermining compliance with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Loss of public trust and concern about use of the app	Privacy by design and default ; Control of security of the phone by the phone and from the operating system provide ; Advice provided to app users in	Accepted	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					privacy notice ; Placed within context of Public Health COVID-19 and manual contact tracing ; Publication of anonymisation, user data journey's and scenarios; Ongoing review of Privacy information						
R011	Malicious or	Proximity	The App	Reputational	Information	Accepted	Sign off on	18-Sep-20	3	3	Amber

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	hypochondriac incorrect self-symptom analysis on app.	users receive false proximity alerts and advice.	does not control accuracy of the data submitted to it.	damage. Undermining purpose of app.	provided within the app and to app users about symptoms and description ; Wider Public Health programme on learning from self-diagnosis ; User Research and feedback programme ; Review of technical controls and issuing of		Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					alerts (limited by data provided by API) ; Ongoing work with Apple/Google regarding Exposure Logging and Notification to manage alerts in a social isolation context ; Advice to contact NHS 111 (or equivalent in Wales) if concerned or for further						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					guidance ;						
R012	Absence of controls over access to app by children (below age range for app)	Inappropriate use by non-competent children resulting e.g. in false self-reported symptoms and proximity alerts.	The App does not control accuracy of the data submitted to it.	Undermining purpose of app.	Controls within the app store allows parents to limit access to the app but this is beyond the control of the organisation ; Users are asked to confirm their age ; Lawful basis for age users with age range (16 to 18) reviewed and	Accepted	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	1	3	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					confirmed ;						
R013	Lower than expected public trust in NHS COVID-19 App	The public do not benefit from the App due to inaccurate reports (or high profile debate about the relative merits of a decentralised -v- centralised model) a suboptimal number of people download the App	Failure to fulfil statutory duties	Risk of damage to the reputation of the organisation and effectiveness of the response to COVID-19.	Extensive comms plan to public , and other stakeholders (inc civil liberties campaigners) to promote trust ; publishing the Privacy Notice , DPIA and source code ; Ongoing information, update and engagement campaign ; Ongoing consultation	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	06-Apr-21	2	3	Amber

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					with Information Commissioner's Office (ICO) ; Ongoing consultation with the National Data Guardian (NDG); Privacy Notice (Young Persons) and Privacy Information (Easy Read); Anonymisation, User Data Journeys						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					and Scenarios						
R014a	There is no mechanism for users see what data deriving from them is held on the app's DHSC secure computing infrastructure database (because it is not possible to relate the data back to individuals)	Users unable to assure themselves that their personal data is not held exercise their other subjects' rights.	None. Article 11(2) applies. For the right to object (Article 21) DHSC should be able to demonstrate compelling legitimate grounds. No data rights are being unreasonably or illegally curtailed	Reputational risk.	As app users are not identifiable within the context of the app data subject rights need to be understood in that context ; Information provided to app users about the use of their data, the limitations on identifiability as part of the	Reduce (Impact)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	06-Apr-21	2	4	Amber

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Privacy Notice ; Where possible users have been given access to the data held on the app with the ability to delete some or all of it app functionality) ; Contents of app and broader comms ; See relevant section of document.						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
R014b	There is no mechanism for users to exercise their rights in relation to personal held on the phone	Users unable to exercise relevant data subject rights (such as Subject Access Requests) as far is applicable	None	Reputational risk	The app allows users to see data it holds, such as the venues that were visited and the timing. There is a function to delete data held on the app, either all or individual venues (management of risks and coercion) ;Data held on the app may only be identifiable	Accepted	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	2	3	Amber

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					to the app user ; Data should be treated as a user held record ; Information provided to app users about the use of their data, the limitations on identifiability as part of the Privacy Notice ; Contents of app and broader comms ; See relevant section of						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					document.						
R015	Uncertainty over retention of individual data items	There is a risk that app users will not know how long their data is to retained at the start of processing	Compliance with Data Protection legislation (if applicable) and broader principles of data storage	Compliance with Data Protection legislation (where applicable), failure to be clear and transparent with app users	Details on retention of data items where known is included in the DPIA and PN (+); Limited identifiability places retention outside of GDPR (but still needs to be set) ; Data items should be considered as a data set to support organisation	Accepted	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	4	1	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					al accountability and retention will reflect this requirement						
R016	Unauthorised disclosure of a user's health status to other app users	Unlawful disclosure resulting in breach of confidentiality and distress to user.	Breach of Article 5(1)(a) – processed lawfully, fairly and in a transparent manner	Vulnerability of organisation to regulatory action and reputational damage.	Diagnosis Keys that are distributed for contact matching do not relate to identifiable individuals ; Secure and privacy preserving method of returning test results to app users ;	Reduce (Impact)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	1	5	Amber

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Clarity in Privacy Notice about potential for potential identifiability outside of the context of the app (i.e. base level risk of public health incidents) ; User Data Journey's and associated scenarios explaining level of risk and impact; Guidance and comms to users						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
R017a	Disclosure by linkage to information held outside the App. (App Environments)	Unlawful disclosure resulting in breach of confidentiality and distress to user.	Breach of Article 5(1)(a) – processed lawfully, fairly and in a transparent manner	Vulnerability of organisation to regulatory action and reputational damage.	Within App: Process of returning results to app users uses single use token and removes identifiability once results are delivered ; data flow to and from app systems break linkage wherever possible ; External to App: Controls around data sets	Reduce (Impact)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	06-Apr-21	1	5	Amber

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					associated with test ordering and test results ; controls within test ordering websites (England) ; Testing process until return of results does not provide the app test code where it is not needed (i.e. before return of results)						
R017b	Disclosure by linkage to information	Unlawful disclosure resulting in	Breach of Article 5(1)(a) –	Vulnerability of organisation	Within NHS Test and Trace Data	Transferred (NHS TTDAP)	Sign off on Risk - Senior Information	06-Apr-21	1	5	Amber

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	held outside the App. (Data held by DHSC)	breach of confidentiality and distress to user.	processed lawfully, fairly and in a transparent manner	to regulatory action and reputational damage.	Analytical Platforms (held by DHSC), see controls within TTDAP to prevent linkage and identification, access control and oversight; Data provided by the app is subject to additional controls before it is provided to TTDAP, data is not user		Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					row level and is subject to additional controls; Ongoing oversight and scrutiny of data flows provided.						
R018	As test ordering requires the submission of directly identifiable information, there should be clear signposting to the user that they are leaving the	Data subjects are not appropriately informed about the controller, purposes for processing, legal basis and other requirements of Articles 12	Non-compliance with DP legislation in particular Articles 12 and 13; reputational damage.	Vulnerability of organisation to regulatory action.	External to App: Privacy Notice, guidance and information to those ordering a virology test via the website ; Privacy statement (	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	1	3	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	App environment.	and 13.			https://test-for-coronavirus.service.gov.uk/appointment); Information about use of data (https://www.gov.uk/government/publications/coronavirus-covid-19-testing-privacy-information.) ; Test ordering user journey provides information prior to app						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					user (or non-app users) submitting data ; Separation out of data sets ;						
R019a	There is a risk the app users can be reidentified by the data held in the product environment (the system that supports the apps functionality and manages the APIs) caused by	Reidentification (impact on privacy and anonymity)	Failure to comply with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Vulnerability of organisation to regulatory action and reputational damage. Loss of public trust.	Privacy by design and default ; Data (analytical data set) collected from user (function specific) are limited and have negligible risk of direct or indirect identification	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	28-Nov-20	0	4	Negligible

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	the data items collected from app users in order to provide them with services.				; The majority of data items within the analytical data set are counts or summaries of interaction with functions of the app not of specific interactions (i.e. a count of venues not of the individual venues accessed) ; Each analytical period only						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					counts interactions within the period and is not cumulative ; The app sends no unique identifier with the analytical data set and no identifier is retained on DH secure data systems ; The process of uploads adds no consistent identifier (by the assigned centrally						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					systems) across analytical data sets ; Controls over access and use within the product environment ; Protections within the APIs and product environment over access and use to data ; Requirements to use Apple Google GAEN limit						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					collection and use of data items from app using their functionality; Add changes or additions to the analytical data set is subject to review, must meet the same criteria and be subject to the same controls;						
R019b	There is a risk the app users can be reidentified	Reidentification (impact on privacy and	Failure to comply with statutory duties and	Vulnerability of organisation to regulatory	Privacy by design and default ; Data	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner	28-Nov-20	0	4	Negligible

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	by the data held in the analytical environment caused by the data items collected from app users in order to provide them with services.	anonymity)	information rights law (GDPR/DP, CLDC, HRA)	action and reputational damage. Loss of public trust.	(analytical data set) collected from user (function specific) are limited and have negligible risk of direct or indirect identification ; The majority of data items within the analytical data set are counts or summaries of interaction with functions of		and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					the app not of specific interactions (i..e a count of venues not of the individual venues accessed) ; Each analytical period only counts interactions within the period and is not cumulative ; The app sends no unique identifier with the analytical data set and						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					no identifier is retained on DH secure data systems ; The process of uploads adds no consistent identifier (by the assigned centrally systems) across analytical data sets ; Controls over access and use within the product environment ; Protections						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					within the APIs and product environment over access and use to data ; Processes of preparation before data is provided to the analytical environment to reduce identifiability ; Postcode District aggregation where postcodes district are particularly small ; Small						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					number suppression engaged where required ; Restriction of data items passed to the analytical environment (postcode district) where reidentificati on is a concern ; No linkage of data at row level from the app to data from any other system ;						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Requirements to use Apple Google GAEN limit collection and use of data items from app using their functionality ; There is active auditing through CDOC for unauthorised access ; Add changes or additions to the analytical data set is subject to review, must						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					met the same criteria and be subject to the same controls;						
R019c	There is a risk the app users can be reidentified by the data held in the product environment's performance viewer (the system that provides dashboards to oversee the	Reidentification (impact on privacy and anonymity)	Failure to comply with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Vulnerability of organisation to regulatory action and reputational damage. Loss of public trust.	Privacy by design and default ; Data (analytical data set) collected from user (function specific) are limited and have negligible risk of direct or indirect identification	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	28-Nov-30	0	5	Negligible

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	performance of the app and the level of use)				; The majority of data items within the analytical data set are counts or summaries of interaction with functions of the app not of specific interactions (i.e. a count of venues not of the individual venues accessed) ; Each analytical period only counts						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					interactions within the period and is not cumulative ; The app sends no unique identifier with the analytical data set and no identifier is retained on DH secure data systems ; The process of uploads adds no consistent identifier (by the assigned centrally						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					systems) across analytical data sets ; Controls over access and use within the product environment ; Protections within the APIs and product environment over access and use to data ; Processes of preparation before data is provided to the performance						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					viewer to reduce identifiability ; Postcode District aggregation where postcodes district are particularly small ; Small number suppression engaged where required ; No linkage of data at row level from the app to data from any other system ;						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Requirements to use Apple Google GAEN limit collection and use of data items from app using their functionality ; There is active auditing through CDOC for unauthorised access ; Robust controls prevent any data export ; Add changes or additions						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					to the analytical data set is subject to review, must meet the same criteria and be subject to the same controls;						
R019d	There is a risk the app users can be reidentified by the data held under the control of the Department for Health and Social	Reidentification (impact on privacy and anonymity)	Failure to comply with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Vulnerability of organisation to regulatory action and reputational damage. Loss of public trust.	Privacy by design and default ; Data (analytical data set) collected from user (function specific) are limited and	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data	06-Apr-21	0	4	Negligible

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	Care (for example, app users who seek a test could be reidentified by combining their data)				have negligible risk of direct or indirect identification ; The majority of data items within the analytical data set are counts or summaries of interaction with functions of the app not of specific interactions (i.e. a count of venues not of the individual venues		Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					accessed) ; Each analytical period only counts interactions within the period and is not cumulative ; The app sends no unique identifier with the analytical data set and no identifier is retained no DH secure data systems ; The process of uploads						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					adds no consistent identifier (by the assigned centrally systems) across 6 hours ; Data from the app is held separately to other data within the Test and Trace programme ; The app associated test code used in the testing process can be used to update a						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					user's status within the app. It is closely managed to prevent the association of anyone receiving testing from the data associated with the app and prevents data from the app being linked to any other data set ; Whilst the testing process will know that						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					someone seeking a test is an app user and can identity that individual, the return of result process ensures that the correct results update the correct app user without being identify which app user or link to any data sets ; The app returns the test						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					result to the correct user but is promptly deleted once validated						
R019e	There is a risk that by collecting a Local Authority and a Postcode District that a user can be reidentified	Reidentification (impact on privacy and anonymity)	Failure to comply with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Vulnerability of organisation to regulatory action and reputational damage. Loss of public trust.	Privacy by design and default ; Data (analytical data set) collected from user (function specific) are limited and have negligible risk of direct or indirect identification	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	29-Nov-20	1	4	Amber

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					; Each analytical period only counts interactions within the period and is not cumulative ; The app sends no unique identifier with the analytical data set and no identifier is retained on DHSC secure data systems ; The process of uploads adds no consistent						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					identifier (by the assigned centrally systems) across analytical data sets ; Controls over access and use within the product environment ; Protections within the APIs and product environment over access and use to data ; Requirements to use						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Apple Google GAEN limit collection and use of data items from app using their functionality ;						
R019f	There is a risk that the Exposure Window data sub-set and Scan Instance data sub-set may make app users or their status identifiable as a result of this data flow	Reidentification (impact on privacy and anonymity)	Failure to comply with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Vulnerability of organisation to regulatory action and reputational damage. Loss of public trust.	Privacy by design and default ; Exposure Window (data set) collected from user is limited and have negligible risk of direct or indirect identification	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	08-Dec-20	0	3	Negligible

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	which may be more vulnerable to network monitoring (which is separate to the analytical data set)				; The data contained within the Exposure Window includes details of interactions but does not contain details of either party involved; The app sends no unique identifier with the Exposure Window data set and no identifier is retained in						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					the DH secure data systems; The Exposure Window is not cumulative or longitudinal and relevant to the period it monitors; The process of uploads adds no consistent identifier (by the assigned centrally systems) across analytical data sets ;						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Controls over access and use within the product environment ; Protections within the APIs, product and analytical environment over access and use to data ; Requirements to use Apple Google GAEN limit collection and use of data items						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					from app using their functionality;						
R019g	There is a risk the app users can be reidentified by the data held under the control of the Department for Health and Social Care in the NHS Test and Trace Data Analytical Platforms (TTDAP) and Joint Biosecurity	Reidentification (impact on privacy and anonymity)	Failure to comply with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Vulnerability of organisation to regulatory action and reputational damage. Loss of public trust.	Controls within the app and the collection of data (see controls listed in Risk R019d); Additional processing and protections within the app data environments prior to provision of data to the TTDAPs; Controls	Transferred (NHS TTDAP)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	06-Apr-21	0	4	Negligible

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	Centre				within the NHS TTDAPs as detailed in the DPIA for that system and the Privacy Notice for Test and Trace						
R020	Absence of controls over access to app by children (age range below 16)	Inappropriate use by children resulting e.g. in false self-reported symptoms and proximity alerts. Risk to the young	The App does not control accuracy of the data submitted to it. Non compliance with statute around use of digital	Undermining purpose of app. Regulatory action, reputational damage and loss of public trust	Controls within the app store allows parents to limit access to the app but this is beyond the control of the organisation	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data	18-Sep-20	2	2	Amber/Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
		app user from use of app where not	services by children (GDPR)		; Users are asked to confirm their age ; Advice provided throughout comms around age of app user ; Age of app user clearly described in published DPIA (DPIA);		Protection Officer				
R021	The app provides services to young app users (age range 16-18). There are	Children's use of the app (age band 16-18) is not supported by appropriate controls	Failure to comply with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Vulnerability of organisation to regulatory action and reputational damage. Loss of	Privacy by design and default within the app ; Young app users are not identifiable outside of	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace	18-Sep-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	additional requirements for data processing for those under the age of 18 (those under 18 are children in GDPR terms)		including those additional points.	public trust.	the data held on the phone within the app ; Provision of additional advise to young app users about differences in wider service (generic) (i.e. show messages to an appropriate adult) ; Legal review of position on PECR, ADM and lawful basis with		programme Sign off for DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					regards to young app users (from 16 to 18 age bracket) ; Consultation with the Information Commissioner's Office						
R022	There is a risk that those functions subject to the Privacy and Electronic Communications Regulations may not meet the	The users may feel that notifications, messages and information associated around the app is intrusive and unrequested	Compliance with PECR [The Privacy and Electronic Communications (EC Directive) Regulations 2003]	Vulnerability of organisation to regulatory action and reputational damage. Loss of public trust.	Privacy by design and default within the app ; data minimisation to support strictly necessary purposes for app user ; clarity on app users	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	1	3	Amber/Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	requirements set out by the regulations and associated legislation.				contribution to Public Health management (COVID-19) ; Legal review of position on PECR and actions taken as a consequenc e ; App Screens, Privacy Notice and DPIA clearly set out functions that fall under PECR and the Public Health						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					function ; Topic included in published DPIA						
R023	There is a risk that those functions, where the standards of Automated Decision Making are noted, may not meet the requirements set out by relevant legislation and guidance	There is a risk that an individual will feel subject to automated decision making that they do not understand, cannot query or disregard	Compliance with Automated Decision Making (ADM, Article 22 of GDPR)	Vulnerability of organisation to regulatory action and reputational damage. Loss of public trust.	Design of the app and supporting services for COVID-19 ensures that human intervention is recommended for all app users when required ; Whilst the app may not fall within the scope of Article 22, it	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	1	3	Amber/Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					seeks to support app users by complying with the requirements of the law and guidance ; Where appropriate, human intervention is recommended to app users at the end of any process with automated decision making ; Publication						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					of explanation of risk algorithm explanation ; Topic included in published DPIA						
R024	Inappropriate use by users (including malicious, erroneous or hypochondriac self-diagnosis app) [Age bracket 16 to 18] see R011	Proximity users receive false proximity alerts and advice.	The App does not control accuracy of the data submitted to it.	Reputational damage, purpose of the app is undermined and public confidence in the app is diminished.	Controls within the app store allows parents to limit access to the app but this is beyond the control of the organisation ; Users are asked to confirm their	Accepted	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	3	2	Amber/Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					age ; Advice provided throughout comms around age of app user ; Age of app user clearly described in published DPIA (DPIA); Information provided within the app and to app users about symptoms and description ; Wider Public Health						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					programme on learning from self-diagnosis ; User Research and feedback programme ; Review of technical controls and issuing of alerts (limited by data provided by API) ; Ongoing work with Apple/Google regarding Exposure Logging and						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Notification to manage alerts in a social isolation context						
R025a	Inappropriate use of the Venue Check-In function (including malicious, erroneous or hypochondriac self diagnosis)	Venue (and attendees) are inaccurately identified as at clinical risk from COVID-19	Failure to upload statutory duties to the public (public health)	Reputational damage, purpose of the app is undermined and public confidence in the app is diminished.	Information provided within the app and to app users about symptoms and description ; Wider Public Health programme on learning from self-diagnosis ; User	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	2	2	Amber/Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Research and feedback programme ; Review of technical controls and issuing of alerts (limited by data provided by API) ; Ongoing work with Apple/Google regarding Exposure Logging and Notification to manage alerts in a social isolation						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					context ; Ongoing programme of public health guidance and comms ; Guidance available in different formats and languages ;						
R025b	Inappropriate use or misleading of the Venue Check-In posters (including malicious creation or faking of QR	App Users are exposed to QR checks posing a risk to the individual's privacy and confidence in the app	Failure to upload statutory duties to the public (public health)	Reputational damage, purpose of the app is undermined and public confidence in the app is diminished.	Process and controls within NHS Official QR creation and use ; Controls within the app to ensure that	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for	18-Sep-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	posters)				only NHS Official QR codes can be scanned ; Support for app users and guidance on official QR codes ;		DPIA - Data Protection Officer				
R026	In order to communicate over the internet address, an IP address is used by mobile phones	The IP address may be associated with individual users	Failure to comply with latest legal position on IP address as identifiable data (Breyer)	Compliance risk, reputational damage, public confidence in the app is diminished	The IP address has to be transmitted by the phone but this is outside of the control of the DHSC ; In line with the Apple Google terms of use,	Accepted	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	4	1	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					the privacy by design and default and commitment to users the IP address is removed from any data packets received at the earliest opportunity and is not retained ; Removal of the IP address is overseen by NCSC, CDOC and the CISO ;						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
R027	The data collected by the app is not proportionate to the purposes that the data is used for	The data collected about individuals is intrusive and is not proportionate to the services provided by the app	Failure to comply with the principles and requirements of information rights law (GDPR, DPA, CLDC and HRA, Article 8)	Compliance risk, reputational damage, public confidence in the app is diminished	Privacy by design and default within app ; Minimal data set with each item and collected reviewed for necessity for purpose ; analytical data set relies on counts and summaries rather than collecting individual items (except postcode district and test result) ;	Reduce (Impact) Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	18-Sep-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					use of data within different environments demonstrates continual minimisation and necessity of data being used						
R028a Interoperability	There is a risk the app users can be reidentified by the data shared through federated servers to support	Reidentification (impact on privacy and anonymity)	Failure to comply with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Vulnerability of organisation to regulatory action and reputational damage. Loss of public trust.	Privacy by design and default ; Requirements to use Apple Google (GAEN) limit collection and use of	Eliminated	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for	17-Oct-20	-	-	N/A

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	alerts to app users across jurisdictions covered by the Interoperability Agreement (Northern Ireland, Scotland, Wales, Jersey, Gibraltar and England)				data items from app using their functionality ; Nature of the diagnosis key as anonymous information ; Interoperability Agreement; Service Level Agreement with Federated Server provider ; Technical Protocol ; Interoperability Governance		DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Group [Name to be confirmed] ; Controls and oversight within Federated Servers of access to data, audit and monitoring ; NB: This risk is similar to any app user with limited social interactions, it also exists with manual contact tracing.						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
R028b Interoperability	There is a risk that app users can be reidentified by the data shared and used to monitor the performance of the interoperability service through federated servers across jurisdictions covered by the Interoperability Agreement (Northern Ireland,	Reidentification (impact on privacy and anonymity)	Failure to comply with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Vulnerability of organisation to regulatory action and reputational damage. Loss of public trust.	Privacy by design and default ; Requirements to use Apple Google (GAEN) limit collection and use of data items from app using their functionality ; Data used to ensure integrity and accuracy of data passed and received from federated servers; Interoperabili	Eliminated	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	17-Oct-20	-	-	N/A

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	Scotland, Wales, Jersey, Gibraltar and England)				ty Agreement; additional of testing type to support appropraite use of Diagnosis Keys in interoperability.						
R028c Interoperability	There is a risk that app users can be reidentified should any data be shared beyond the partners to the interoperabili	Reidentification (impact on privacy and anonymity)	Failure to comply with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Vulnerability of organisation to regulatory action and reputational damage. Loss of public trust.	Privacy by design and default ; Requirements to use Apple Google (GAEN) limit collection and use of data items	Eliminated	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data	17-Oct-20	-	-	N/A

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	ty agreement should a partner provide data shared onto additional bodies				from app using their functionality ; Data used to ensure integrity and accuracy of data passed and received from federated servers; Interoperability Agreement Service Level Agreement with Federated Server provider ; Technical Protocol ;		Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Interoperability Governance Group [Name to be confirmed] ; Controls and oversight within Federated Servers of access to data, audit and monitoring ; Minimisation of data used to monitor services						
R029 Interoperability	There is a risk for app users with	Reidentification (impact on privacy	Undermining compliance with	Loss of public trust and concern	Privacy by design and default (-);	Accepted	Sign off on Risk - Senior Information	17-Oct-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	limited social interactions that they might be identifiable or be able to identify other app users due to these limited social interactions	and anonymity)	statutory duties and information rights law (GDPR/DP, CLDC, HRA)	about use of the app	Requirements to use Apple Google (GAEN) limit collection and use of data items from app using their functionality (-); Advice provided to users about risks of identification outside of the app (-); Privacy Notice (-); Interoperability Agreement (-);		Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Memorandum of Understanding between parties (-); Service Level Agreement with Federated Server provider (-); Technical Protocol (-); Interoperability Governance Group [Name to be confirmed] (-)						
R030	Uncertainty	There is a	Undermining	Loss of	Interoperabili	Reduce	Sign off on	17-Oct-20	4	1	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
Interoperability	over retention of diagnosis keys across jurisdictions they are shared with	risk that app users will not know how long their data is to be retained at the start of processing	compliance with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	public trust and concern about use of the app	ty Agreement (MOU) Service Level Agreement with Federated Server provider ; Technical Protocol ; Interoperability Governance Group [Name to be confirmed] ; Clear agreement of Diagnosis Keys storage on Federated	(Likelihood)	Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Server ; Alignment of retention of diagnosis keys across jurisdictions within interoperability agreement ; Privacy Notice details retention of Diagnosis Keys for users across interoperability agreement						
R031 Interoperability	There is a risk that diagnosis keys passed	There is a risk that once a diagnosis	Undermining compliance with statutory	Loss of public trust and concern about use of	Privacy by design and default ; Requirement	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner	17-Oct-20	3	1	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	to other jurisdictions may be shared further without the app user's permission or being informed	key is outside of the control of the data controller they may be shared further than expected	duties and information rights law (GDPR/DP, CLDC, HRA)	the app	s to use Apple Google (GAEN) limit collection and use of data items from app using their functionality ; Interoperability Agreement ;Service Level Agreement with Federated Server provider ; Technical Protocol ; Interoperability		and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Governance Group [Name to be confirmed] ; Clear agreement of Diagnosis Keys storage on Federated Server						
R032 Interoperability	There is a risk that data provided or derived from data provided by England and Wales are not subject to robust controls	None identified	Undermining public trust, compliance and England and Wales ability to oversee information	There is a risk that the data supporting the exchange of diagnosis keys, or that could be derived from them - such	Limitations of data item and data that can be derived from it; Interoperability Agreement ; Service Level	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data	17-Oct-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	once downloaded by other jurisdictions.			as a count of Diagnosis Keys, will not be under the control of England and Wales once they are shared with other jurisdictions	Agreement with Federated Server provider ; Technical Protocol ; Interoperability Governance Group [Name to be confirmed] ;		Protection Officer				
R033 Interoperability	Lack of technical or organisational measures implemented to ensure appropriate security of the data on the	Risk to individuals arising from inadequate technical or organisational controls to protect the data. Data breach due	Non-compliance with statutory obligations	Potential for regulatory investigation and subsequent action; reputational damage and loss of trust from app	Privacy by design and default ; Requirements to use Apple Google (GAEN) limit collection and use of	Reduced (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for	17-Oct-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	federated servers or once passed to other jurisdictions	to technical weakness (e.g. cyber-attack); access by unauthorised people.		users	data items from app using their functionality ; Interoperability Agreement ; Service Level Agreement with Federated Server provider ; Technical Protocol ; Interoperability Governance Group [Name to be confirmed] ; Controls and		DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					oversight within Federated Servers of access to data, audit and monitoring ; PEN and Cyber Security testing of Federated Server ; Exchange of Cyber Security Assurance between parties						
R034 Interoperability	There is a risk that app users who	Failure to provide an effective	Failure to uphold statutory	Loss of public trust about the	Provision of interoperability across	Reduced (Likelihood)	Sign off on Risk - Senior Information	17-Oct-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	live and work on the border of different jurisdictions are not supported by the NHS COVID-19 app	service and accurate information for app users across jurisdictions	obligations towards citizens	value and efficacy of the app	jurisdictions set out in the interoperability agreement		Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer				
R035 Interoperability	There is a risk that app users who travel between countries are not supported by the NHS COVID-19 app	Failure to provide an effective service and accurate information for app users across jurisdictions	Failure to uphold statutory obligations towards citizens	Loss of public trust about the value and efficacy of the app	Provision of interoperability across jurisdictions set out in the interoperability agreement	Reduced (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection	17-Oct-20	2	2	Amber/Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
							Officer				
R036 Interoperability	There is a risk that diagnosis keys are not in the correct format, shared and utilised to the maximum benefit of users	Failure to provide an effective service and accurate information for app users across jurisdictions	Failure to uphold statutory obligations towards citizens	Loss of public trust about the value and efficacy of the app	Work of Interoperability Governance Group ; Technical Protocol ; Synchronisation of Servers ; Procedures within NHS COVID-19 app programme to ensure accuracy and validity of submissions ; Procedures within NHS	Reduced (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	17-Oct-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					COVID-19 app to support accuracy and validity of keys received from other jurisdictions						
R037	There is a risk that app users may be able identify venues that are the source of an alert	Loss of personal data to non-trusted sources; privacy risk due unauthorised sharing of personal data. Venue (and attendees)	Non-compliance with data protection legislation.	Reputational risk. Failure to fulfil obligations towards venues and app users. Vulnerability of organisation to regulatory action and reputational	No details are provided about venues in alerts; details in the alerts limit the ability to identify any venue from the alert; Risks are broadly in	Accepted	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	08-Dec-20	1	3	Amber/Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
		are inaccurately identified as at clinical risk from COVID-19		damage.	line with wider contact tracing and health protection team venue/site interventions						
R038	There is a risk that app users will not know their Local Authority and may not be entered correctly	The individual may not get the relevant information for their area (risks, testing options and services)	Failure to comply with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Reputational risk. Failure to fulfil obligations towards app users. Vulnerability of organisation to regulatory action and reputational damage.	The app will support the app user in selecting the relevant local authority after adding postcode district, there is additional support available from the	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	29-Nov-20	1	2	Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					gov.uk; advice to user. Information is available from multiple sources to support.						
R039	There is a risk that collecting both postcode district and Local Authority is not in line with the principle of data minimisation	There is a risk that an individual may be more identifiable due the collection of Local Authority and postcode district	Failure to comply with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Vulnerability of organisation to regulatory action and reputational damage. Loss of public trust.	Privacy by design and default ; Data (analytical data set) collected from user (function specific) are limited and have negligible risk of direct	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	28-Nov-30	1	3	Amber/Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					or indirect identification ; The majority of data items within the analytical data set are counts or summaries of interaction with functions of the app not of specific interactions (i.e. a count of venues not of the individual venues accessed) ; Each analytical						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					period only counts interactions within the period and is not cumulative ; The app sends no unique identifier with the analytical data set and no identifier is retained on DH secure data systems ; The process of uploads adds no consistent identifier (by						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					the assigned centrally systems) across the collection period ; Controls over access and use within the product environment ; Protections within the APIs and product environment over access and use to data ; Requirements to use Apple Google						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					GAEN limit collection and use of data items from app using their functionality; Add changes or additions to the analytical data set is subject to review, must met the same criteria and be subject to the same controls						
R040 Support	There is a risk that the	Reidentificati on (impact	Failure to comply with	Reputational risk. Failure	Within the app context	Reduce (Likelihood)	Sign off on Risk - Senior	07-Dec-20	0	4	Negligible

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
Isolation Payment	app users seeking Self-Isolation Payment, when recommended, will be identifiable within the app's data sets.	on privacy and anonymity)	statutory duties and information rights law (GDPR/DP, CLDC, HRA)	to fulfil obligations towards app users. Vulnerability of organisation to regulatory action and reputational damage.	Data and Privacy page in the app; Information provided on Self-Isolation pages and process; Privacy Notice for the app ; Communication campaign for public about app and Self-Isolation Payments ; O; Publishing DPIA ; The IPC token created provides the		Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer				

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					link from the app to Gateway portal. Once the app user is confirmed as a resident of England, the encounter date and isolation end date is the only data to be pulled through from the app. This approach takes the same privacy by design method as						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					per the book a test journey to ensure the app user's anonymity is preserved. Within the portal and self-isolation claim process. Information provided to the applicant about the process, the obligations upon them and the requirements for claiming the Self-Isolation						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					Payments. For more information see the risk register for the self-isolation process.						
R041 Support Isolation Payment	There is a risk that app users seeking Self-Isolation Payment will not be aware of the obligations that seeking Self-Isolation Payments put upon them.	The app user may face legal consequences from applying for Self-Isolation Payments but not understanding the requirements.	Failure to comply with statutory duties and information rights law (GDPR/DP, CLDC, HRA)	Reputational risk. Failure to fulfil obligations towards app users. Vulnerability of organisation to regulatory action and reputational damage.	Within the app context: Data and Privacy page in the app; Information provided on Self-Isolation pages and process; Privacy Notice for the app ; Communicati	Transferred (Self-Isolation Process)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and Trace programme Sign off for DPIA - Data Protection Officer	07-Dec-20	1	4	Amber

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					on campaign for public about app and Self-Isolation Payments ; O; Publishing DPIA ; Within the portal and self-isolation claim process Information provided to the applicant about the process, the obligations upon them and the requirements for claiming						

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
					the self-isolation payments. The user is required to provide their agreement to proceed. For more information see the risk register for the self-isolation process.						
R042	There is a risk that the app is not presenting choices in a fair and transparent	There is a risk that individuals are not given a fair choice	Non-compliance with data protection legislation and obligations	Reputational risk. Failure to fulfil obligations towards app users. Vulnerability	Provision of choices to app users throughout the user journey for user choice;	Reduce (Likelihood)	Sign off on Risk - Senior Information Risk Owner and Chief Executive for Test and	06-Apr-21	2	2	Amber/Green

Risk reference (Ver 0.2): A unique coding that allows the risk to be easily identified	Privacy issue – element of the initiative that gives rise to the risk	Risk to individuals (complete if appropriate to issue or put not applicable)	Compliance risk (complete if appropriate to issue or put not applicable)	Associated organisation/corporate risk (complete if appropriate to issue or put not applicable)	Proposed solution(s)/ mitigating action(s) – systems and processes that are or will be in place and operating that mitigate this risk, including assurances	Result, is the risk accepted, eliminated, or reduced?	Risk to individuals is now acceptable? Signed off by?	Date for completion	Likelihood	Impact	RAG status
	manner for app users			of organisation to regulatory action and reputational damage.	Ability to change choices and to say no; FAQs, published Privacy Notice and Data Protection Impact Assessment (DPIA); Ongoing communications and engagement with the public and app users.		Trace programme Sign off for DPIA - Data Protection Officer				

Section 8: Document Sign off

Business lead: Gaby Appleton, Product Director, NHS COVID-19 app

Data owner: David Williams (Deputy, Lorraine Jackson), 7 December 2020

IT business partner: Barry McCormack

DPO: Lee Cramp, 7 December 2020

Appendices to this DPIA

Appendix 1 – data dictionary

This section lists the data that is produced by the app system. It is divided into 2 sections:

- operational data
- data supporting interoperability (working with other health service digital contact tracing apps)
- analytical data
- event analytical data

Additional details are provided about:

- Exposure Window Data Set and Scan Instance Data Sub-set
- Isolation Status and Reason
- Test Status and Test Process

In addition, a note is made of data used to support Isolation Support Payments.

For the purpose of this document data can live on the iOS or Android app (App) or the app specific backend DHSC secure computing infrastructure (Cloud).

Operational data

This is data collected by the app during its normal operation.

Name	Description	Capture	Processing	Distribution	Lifespan	Benefit of processing
Contacts Detected	Contacts detected inside the GAEN	Apple / Google EN API	Not available for processing	Within the OS, not accessible to the App	Completely managed by Apple/Google	Not applicable
Exposure Events	Matches between Positive Keys and Contacts Detected. Never discloses the user that was matched Note: only relevant to GAEN Mode 1	Apple/Google GAEN, when a contact match is made	Aggregated on the cloud platform to provide statistics	Generated on the App, shared with Cloud	Short. From match detection until aggregated into statistics	Statistics on matches being made are critical to understand and improve the performance of the contact matching configuration
Exposure Windows	Where a match between a Diagnosis Key and Contact is detected an Exposure Window is generated which captures the details used to determine if an app user is alerted. Never discloses the user that was matched. Note: only relevant to GAEN Mode 2	Apple / Google EN API, when a contact match is made	The app uses this information to identify if the app user has been exposed to a positive contact and to calculate the risk of infection	Generated on the App, shared with Cloud	Short. Aligned with the period the Isolation Countdown is Active	Statistics on matches being made are critical to understand and improve the performance of the contact matching configuration
Exposure Matches	Matches between diagnosis keys and broadcast codes. Includes whether the	Apple/Google GAEN, when a contact match is made and relevant	Aggregated on the product environment to provide statistics	Collected in app and passed to app back-end	Short. From match detection until aggregated into	Statistics on matches and their nature being made are critical to understand and improve

Name	Description	Capture	Processing	Distribution	Lifespan	Benefit of processing
	match was above or below the risk threshold. Never discloses the user that were matchated.	Exposure Window data set		(product environment)	statistics	the performance of the contact matching configuration
Test status, type and test process	Results of testing, test type and process.	NPEx (National Pathology Exchange) National Test Database, which is passed the data by the Testing Labs	Distributed to all app instances	Passed to the Cloud by 3rd party. Shared will all App instances.	As long as the app is installed	Essential to determine which app users are positive index cases and the test process used (i.e. whether the test process started and ended in the app) Where applicable will recommend the user seeks a confirmatory test after a first test result.
Onset of Symptoms	The data around when the app user shows symptoms	The date is captured when the user populates the symptoms questionnaire	The app uses this information to calculate the isolation countdown timer and identify the period which the app user is an index case	Stored on the App. Not Distributed	14 days	Essential to determine the appropriate isolation window for users and appropriate window a user is an index case for exposure detection This is collected via the app or alternatively via the testing route, where appropriate.
Diagnosis Key Sets	Diagnosis Keys from the GAEN that are requested when a user is confirmed positive and shared with other users.	Apple/Google GAEN, when a suspected positive user is requested to submit their keys	A transmission risk is added to the key set before it is sent to the cloud.	Generated on the App, stored on Cloud. Sent to all App instances	14 days.	Essential that these keys are distributed to all participating apps as they are the data that is matched against to

Name	Description	Capture	Processing	Distribution	Lifespan	Benefit of processing
	This references data items that enables the infectiousness of the contact to be calculated.					identify contacts with index cases
QR Venues Visited	QR codes derived from scanning QR images	Captured using phone's camera QR code scanning function under full app control	QR code is decoded to capture venue identifiers, including venue post and stored encrypted on the phone.	Generated on the App. Never shared.	21 days	Used to match Hot Spot Venue codes
Hotspot QR Venues	QR codes for venues that could have caused users to become infected	Identified outside of the app system by Manual Contact Tracing teams	Used with the app to look for matches identifying when an app user has visited a hotspot location.	Passed to the Cloud by 3rd party. Shared will all App instances.	21 days	Used to match visited venue codes
Postcode district	First half (2 to 4 digits) of Post Code prior to the space	Entered by the app user in app onboarding sequence	Stored on the app securely. Included in analytics when transmitted anonymously to the cloud	Stored on the App. Shared with Cloud with Analytics	As long as the app is installed	Enables system to present captured statistical data on a regional basis, to understand behaviour and infection rates in specific areas. Allows for user to be presented with local information such as infection risk, additional testing or

Name	Description	Capture	Processing	Distribution	Lifespan	Benefit of processing
						services available in an area.
Local Authority	Based on the postcode district entered by the user	Selected by the app user and based upon the postcode district entered in the app onboarding sequence	Stored on the app securely. To be included in analytics when transmitted anonymously to the Cloud	Stored on the App. Shared with Cloud with Analytics	As long as the app is installed	Enables system to present captured statistical data on a regional basis, to understand behaviour and infection rates in specific areas. Allows for user to be presented with local information such as infection risk, additional testing or services available in an area.
Area Risks	Infection Risk Level for an area (either postcode district or local authority). See Note 1	Published by the Joint Biosecurity Centre	Distributed to all app instances	Passed to the Cloud by 3rd party. Shared will all App instances.	As long as the app is installed	Allows for the user to be presented with infection risk for local area and other areas. Whether this is by Local Authority or Postcode District is determined by the latest public health policy.
Test status and test process	Results of Testing	NPEx (National Pathology Exchange) National Test Database, which is passed the data by the Testing Labs	Distributed to all app instances	Passed to the Cloud by 3rd party. Shared will all App instances.	As long as the app is installed	Essential to determine which app users are positive index cases and the test process used (i.e. whether the test process started and ended in the app)

Name	Description	Capture	Processing	Distribution	Lifespan	Benefit of processing
Isolation status and reason	Record of the Isolation and the rationale	Captured from the trigger for the self-isolation recommendation	Stored on the app securely. To be included in analytics when transmitted anonymously to the cloud	Stored on the App. Shared with Cloud with Analytics	Short. Aligned with the period the Isolation Countdown is Active	To set the isolation countdown accurately and to record the reason the user was recommended to self-isolate
Isolation Support Payment Function	Data collection about the generation and use of the Isolation Support Payment Function	Generated within the app	Stored in app and in app back-end.	Collected in app and passed to app back-end (product environment)	Within app, aligned with duration of isolation period	Essential to validation of isolation support payment function.

Interoperability data (supporting operational functions)

The following data item supports working with other health service digital contact tracing apps.

Name	Description	Capture	Processing	Distribution	Lifespan	Benefit of processing
Diagnosis Key Sets	Diagnosis Keys from the GAEN that are requested when a user is confirmed positive and shared with other users This does not include references data items that enables the infectiousness of the contact to be calculated.	Apple/Google GAEN, when a suspected positive user is requested to submit their keys	Whilst a transmission risk is associated with the Key before use within the NHS COVID-19 app systems it will not be shared for interoperability at this stage.	Provided to the Federated Server for other jurisdictions within the interoperability agreement to utilise to pass on to their app users. Functionality controlled by GAEN.	14 days.	Essential that these keys are distributed to all participating apps as they are the data that is matched against to identify contacts with index cases

The point of origin, jurisdiction, can be inferred from the diagnosis keys; it is expected that this will help monitor the performance and accuracy of the interoperability service.

The diagnosis key is necessary for this function. It supports the 1. Get notified and 6. Support public health and understanding of COVID-19.

Analytics data

Note: For this release the analytical data set was reviewed.

This is data which is collected explicitly for the purpose of understanding the performance of behaviour of the app system.

Analytics data table

The table below details the proposed data fields send out by the app in the analytic packets

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve?	Necessary or Discretionary?	Which benefit of the app does it support?
Period	Records the start and end date of the analytical period	Recorded by the app daily, Automatic	Sent to the Cloud with other stats, then aggregated into summary statistics	As analytical data packets are sent across a daily period, it ensures that the stats are attributed to the correct period.	Aggregated in to summary statistics, which are then maintained as long as the app system is operational	Supports the accuracy of data and analysis by correctly attributing data items to the correct period.	Required across all uses to ensure data is appropriately attributed	Necessary	1,2,3,4,5, 6
Postcode District	First half (2 to 4 digits) of Post Code, before the space	Entered by the app user in app onboarding sequence. Text string	Sent to the Cloud with other stats, then aggregated into summary statistics	Used to understand data differences on a regional basis	Aggregated in to summary statistics, which are then maintained as long as the app system is operational	Enables system to present captured statistical data on a regional basis, to understand behaviour and infection rates in specific areas.	Public Health. Understand regional variations. Predict a R increase before it happens	Necessary	1,6
Local Authority	Based on the postcode district entered by the user	Selected by the app user and based upon the postcode district entered in the app	Sent to the Cloud with other stats, then aggregated into summary statistics	Used to understand data differences on a regional basis	Aggregated into summary statistics, which are then maintained	Enables system to present captured statistical data on a regional basis, to understand behaviour and infection rates in	Public Health. Understand regional variations. Predict a R increase before it happens.	Necessary	1,6

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve?	Necessary or Discretionary?	Which benefit of the app does it support?
		onboarding sequence			as long as the app system is operational	specific areas.			
Phone Model	Device type as reported by the operating system	Reported by phone OS as text string	Sent to the Cloud with other stats, then aggregated into summary statistics	Used to understand phone types the app is deployed to	Aggregated into summary statistics, which are then maintained as long as the app system is operational	Enable understanding of what mobile devices need to be supported, and if particular devices are behaving differently	Analysis. Determine issues with specific mobile devices. Medical device requirement Too many different phone models for a portion of this to be effective.	Necessary	1,2,3,4,5, 6
Operating System Version	The version number of the phone operating system	Reported by phone OS as text string	Sent to the Cloud with other stats, then aggregated in to summary statistics	Used to understand phone OS versions the app is deployed to	Aggregated in to summary statistics, which are then maintained as long as the app system is operational	Enable understanding of what phone OSs need to be supported, and if particular OS versions are behaving differently	Analysis. Determine issues with specific mobile device versions. Medical device requirement Many different operating system versions. Supports device investigation.	Necessary	1,2,3,4,5, 6
App Version Number	The version number of the app release	Reported by the App as text string	Sent to the Cloud with other stats, then aggregated in to summary	Used to understand how many users have not upgraded to	Aggregated in to summary statistics, which are then	Used to direct what comms or nudges are needed to encourage users to upgrade	Analysis. Determine issues with specific app versions, and problems with users not	Necessary	1,2,3,4,5, 6

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve?	Necessary or Discretionary?	Which benefit of the app does it support?
			statistics	the latest version	maintained as long as the app system is operational		upgrading. This is important because if we find defects, we want to know how many people are still running on old version to minimise their risk. Post market surveillance. Medical device requirement		
Onboarding Completed	How many users have not only installed the app but completed the onboarding process	Reported by the App as an event	Sent to the Cloud with other stats, then aggregated in to summary statistics	Used to understand how many users have installed and onboarded with the app	Aggregated in to summary statistics, which are then maintained as long as the app system is operational	User to understand how many users install the app but then choose not to complete onboarding	Public Health. Understand how many users have installed the app. App store tells us how many have downloaded the app. This data tells us how many have enabled it. This is a safety issue to ensure people don't think they have protection that they do not have. Medical device requirement	Necessary	1,2,3,4,5,6
Usage Status	How many hours the app has been active/running on the phone in the	Captured within App as hour counts	Sent to the Cloud with other stats, then	Used to contact active users and	Aggregated in to summary statistics,	Used to understand how many of the population are actively using the	Public Health. Understand how many users are actively using the	Necessary	1,2,3,4,6

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve?	Necessary or Discretionary?	Which benefit of the app does it support?
	past 24 hours		aggregated in to summary statistics	understand whether the app is running all 24 hours as expected	which are then maintained as long as the app system is operational	app, and if further promotion is needed/proving effective	app. The technology will wake the phone up every 2 hours to check the latest information has been downloaded. This data ensures contact tracing is on and working, that they are being protected. This will highlight if the technology is not working on phones.		
Storage Usage	How many bytes of persistent phone storage are we using	Measured by asking phone OS as integer byte count	Sent to the Cloud with other stats, then aggregated into summary statistics	Used to understand how much of the phone's storage data is in use	Aggregated into summary statistics, which are then maintained as long as the app system is operational	Used to understand if the app is causing problems due its data storage requirement, and what action might be needed	Analysis. Understand data storage issues. Important for equalities as older phones will have less storage available. This will ensure we understand where storage may be problematic.	Necessary	1,2,3,4
Data Download Usage	In the past 24 hours how many bytes of data were downloaded and uploaded by the device. Cumulative	Measured by asking phone OS as integer byte count	Sent to the Cloud with other stats, then aggregated in to summary	Used to understand how much of the phones download data is being	Aggregated in to summary statistics, which are then	Used to understand if the app is causing problems due its data download requirement, and what action might be	Analysis. Understand data download issues. Important for equalities to ensure understanding data	Necessary	1,2,3,4

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve?	Necessary or Discretionary?	Which benefit of the app does it support?
	Upload and Download, divided across Wi-Fi and Mobile (Cellular) data.		statistics	used	maintained as long as the app system is operational	needed	usage.		
Exposure Events Note: only relevant to GAEN Mode 1	Matches between Positive Keys and Contacts Detected. Never discloses the user that was matched. Includes Duration, Attenuation (as a proxy for distance) and the resulting risk score.	Apple / Google EN API, when a contact match is made	Aggregated on the Cloud platform to provide statistics	Generated on the App, shared with Cloud	Short. From match detection until aggregated in to statistics	Statistics on matches being made are critical to understand and improve the performance of the contact matching configuration	Understand that matches are being made at expected levels. This allows us to understand the accuracy of the isolation advice. Foundation technology Relates to public health and the standard of service provided to the user.	Necessary	1, 6
Exposure Windows See below for the full details of the Exposure Window date set Note: only relevant to GAEN Mode 2	Where a match between a Diagnosis Key and Contact is detected an Exposure Window is generated which captures the details used to determine if an app user is alerted. Never discloses the user that was matched.	Apple / Google EN API, when a contact match is made and an Exposure Window is generated [related to the event]	Aggregated on the Cloud platform to provide statistics	Generated on the App, shared with Cloud	Short. From match detection until aggregated into statistics	Statistics on matches being made are critical to understand and improve the performance of the contact matching configuration	Understand that matches are being made at expected levels. This allows us to understand the accuracy of the isolation advice. Foundation technology Relates to public health and the standard of service provided to the user.	Necessary	1, 6
Pause Usage	How many times a day, and for how	Captured within App as	Sent to the Cloud with	Used to understand	Aggregated in to	Understand value to users and usage of	Delivery of Service. Understand for how	Necessary	1, 6

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve?	Necessary or Discretionary?	Which benefit of the app does it support?
	long the pause button is used to disable contact tracing	integer counts	other stats, then aggregated in to summary statistics	how much time the app is in an idle state	summary statistics, which are then maintained as long as the app system is operational	this feature.	long users are actively using the app. Necessary for public health to be able to check that app is still active.		
QR Code Check-in Counts	Count of QR check-ins logged by the phone	Captured within App as integer check-in count	Sent to the Cloud with other stats, then aggregated in to summary statistics	Used to understand whether the app is capturing the number of QR check-ins expected	Aggregated in to summary statistics, which are then maintained as long as the app system is operational	Informs programme on whether QR code programme is operating well, and what management actions are required	Analysis. Understand that check-ins are being made at expected levels. Extent to which we can alert people if venues are risky. Understanding the true level of risk i.e. are people not checking into risky venues vs they are not checking in venues at all.	Necessary	2, 6
Symptomatic Questionnaire Results	Result of the symptomatic questionnaire (suspected positive or not)	Captured within App as result of questionnaire submission	Sent to the Cloud with other stats, then aggregated in to summary statistics	Used to understand what % of users (and wider population) are thought to have covid like	Aggregated in to summary statistics, which are then maintained as long as the app	Enables future infection, testing and health provision to be predicted, helping to manage healthcare provision	Public Health. Understand symptom results of users. This is the advice given to a user based on the symptom questionnaire (isolate or not	Necessary	3,5, 6

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve?	Necessary or Discretionary?	Which benefit of the app does it support?
				symptoms	system is operational		isolate). Medical device requirement		
Isolation Status and Reason For more details on the data items within this data set see below	Whether/how the user has been asked to isolate, and whether this is due to self-diagnosis, test result, or exposure notification.	Captured within App as structured data capturing the current isolation status	Sent to the Cloud with other stats, then aggregated in to summary statistics	Used to understand what % of users (and wider population) are isolating	Aggregated in to summary statistics, which are then maintained as long as the app system is operational	Gauge impact of app in isolating potentially infectious users, a key success measure for the app	Analysis. Understand that isolations are being requested as expected. This is a public health point around how many people have been asked to stay home and where are they. Medical device requirement as output from symptomatic Questionnaire	Necessary	4,5, 6
Test Status and Test Process For more details on the data items within this data set see below	When the user has been recommended to take a test, what the result was, and why we recommended them (self-diagnosis or exposure notification). Also captures the testing journey, to help ensure this is scrutinized and forms part of the analysis undertaken	Captured within App as structured data capturing test results	Sent to the Cloud with other stats, then aggregated in to summary statistics	Used to understand how users have tested, which can be compared to what direction the app gave them	Aggregated in to summary statistics, which are then maintained as long as the app system is operational	Gauge impact of app in helping users get access to tests and identifying infectious individuals	Analysis. Understand how symptoms submitted or contact matches made relate to test results. If we have told someone to isolate because of questionnaire response or contact match, then we would need to understand their test result to measure to efficacy	Necessary	4, 5, 6

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve?	Necessary or Discretionary?	Which benefit of the app does it support?
							of the system. Medical device requirement as output from symptoms Questionnaire		
Isolation Support Payment Function	Counts of the use Isolation Support Payment function	Generated within the app with the use of Isolation Support Payment	Sent to the Product Environment with other stats, then aggregated into summary statistics	As analytical data packets are sent across a daily period, it ensures that the stats are attributed to the correct period.	Aggregated in to summary statistics, which are then maintained as long as the app system is operational	Essential to the validation of the Isolation Support Payment function	Required for purpose of monitoring functions and analysis of use of service	Necessary	6
Exposure Matches	Counts the number of risky and non risky matches between Diagnosis Keys and Broadcast Codes	Generated within the app and part of the GAEN function.	Sent to the Product Environment with other stats, then aggregated into summary statistics	As analytical data packets are sent across a daily period, it ensures that the stats are attributed to the correct period.	Aggregated in to summary statistics, which are then maintained as long as the app system is operational	Essential to the maintaining the notification service and understanding of the exposure window functionality.	Required for purpose of monitoring functions and analysis of use of digital contact tracing	Necessary	1, 6
User Notification Analytics	Counts whether the user has responded to an Notification, provides a measure	Generated within the app and as part of the GAEN	Sent to the Product Environment with other	As analytical data packets are sent across a	Aggregated in to summary statistics,	Essential to the monitoring the notification service and the impacts	Delivery of Service. Understand impact and value of alerts ot users.	Necessary	1, 6

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve?	Necessary or Discretionary?	Which benefit of the app does it support?
	of the time taken to respond and measures the impact	function.	stats, then aggregated into summary statistics	daily period, it ensures that the stats are attributed to the correct period.	which are then maintained as long as the app system is operational	upon app users.	Necessary for public health to determine value and impact of alerts.		
Confirmatory Testing Analytics	Counts whether a user has received and/or responded to a confirmatory test recommendation from the app.	Generated within the app as part of the testing result journey	Sent to the Product Environment with other stats, then aggregated into summary statistics	As analytical data packets are sent across a daily period, it ensures that the stats are attributed to the correct period.	Aggregated in to summary statistics, which are then maintained as long as the app system is operational	Essential to the monitoring the testing process and the use of the confirmatory testing journey.	Delivery of Service. Understand impact and value of alerts to users. Necessary for public health to understand impacts of confirmatory testing.	Necessary	1, 6
Isolation Period Support Analytics [Onset Symptoms Date]	Counts when a user is prompted to enter an onset of symptoms date, whether symptoms are added and a note on whether they occurred before a test result was received.	Generated within the app as part of the testing result journey.	Sent to the Product Environment with other stats, then aggregated into summary statistics	As analytical data packets are sent across a daily period, it ensures that the stats are attributed to the correct period.	Aggregated into summary statistics, which are then maintained as long as the app system is operational	Essential to monitoring the function of the app, ensuring that users receive the isolation advice in line with the latest guidance. Supports public health and understanding of COVID-19 by ensuring that all users have an opportunity to enter an onset of	Delivery of Service. Enables public health understanding include relationship between testing and symptoms	Necessary	4, 6

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve?	Necessary or Discretionary?	Which benefit of the app does it support?
						symptoms date. By understanding when no symptoms are recorded or noted supports greater understanding of testing and symptoms by app users.			

Isolation Support Payment Function: Data Items

Data Item	Description
have Active Ipc Token	This is a count of whether devices are displaying the financial support button (this is triggered once the exposure notification event has happened). The button will appear on the device for the duration of their isolation period.
received Active Ipc Token	This is a count of whether the device displayed the financial support button for the first time on a given day. This differs from the above as have Active Ipc Token counts every device displaying the button which appears over a 14 day period. This allows us to validate that the service is working
tapped Isolation Payments Button	This is a count of whether a device has clicked the financial support button.
launched Isolation Payments Application	This counts whether the device has launched the Isolation Payment application. It will be important to ensure the count of tapped Isolation Payments Button (i.e. the number of devices which have triggered the financial support button) this figure to ensure the number of devices which trigger the process to launch into the Gateway portal. If these numbers are different proactive trouble shooting can be conducted to determine any technical issues. This allows us to validate the service is working correctly.

User Notification Analysis

The following data items are added to the analytical data set collected each day.

Data Item	Description
acknowledged Start Of Isolation Due To Risky Contact	[Exposure Notification Acknowledged] Adds a count of if the user has acknowledged the exposure notification and used to understand if an exposure notification is viewed and acknowledged. Enables the public health impacts of the notifications to be understand and a measure of the effectiveness of the service.
has Notifications Enabled Background Tick	[Notifications enabled] Adds a count if the user has enabled notifications for the app, captured from the apps current setting. Used to understand if the app is enabled to raise notification's. Helps measure whether the users are engaged with the Digital Contact Tracing service, as well as understanding the public health impacts and potential.
total Risky Contact Reminder Notifications	[Reminder Exposure Notifications] Counts the number of how many reminder exposure notifications were raised during the daily analytical period. User to understand the public health impacts of the notifications and monitor the service. Helps monitor technical issues around Exposure Notification and user alerts across Apple and Google systems.

Confirmation Testing Analysis

The following data items are added to the analytical data set collected each day.

Data Item	Description
received Unconfirmed Positive Test Result	Counts when a positive test result with a test type that requires confirmatory testing is entered by the user or received by the app via the Testing API
is Isolating For Unconfirmed Test Background Tick	Counts when a user has received a positive test result, from a test type that requires confirmation, and is advised to self-isolation
launched Test Ordering exposure notifications	Notes if the user has launched the Test Ordering exposure notifications function around requiring a confirmatory test.

Isolation Period Support and Analytics [related Onset of Symptoms Date]

The following data items are added to the Analytical Data Set in order to: (a) ensure the function is working as expected and to (b) improve the public health understanding from the details entered by app users.

Data Item	Description
Symptoms requested [Technical Description: Did Ask For Symptoms On Positive Test Entry]	This counts if the app displays the screen asking the user if they have symptoms after receiving a positive COVID-19 test
Symptoms noted [Technical description: Did Have Symptoms Before Received Test Result].	A count which is increased when a user selects yes when asked if they have symptoms. This works alongside the other data items to help ensure the user has received the correct advice, the service is working as expected.
Symptoms onset date entered [Technical description: Did Remember Onset Symptoms Date Before Received Test Result].	This data item counts when the app user enters a symptom start date into the field. Please note: it does not capture details of the date, just that one was entered.

Event Analytical Data Set(s)

The following data is related to specific events and is processed outside of the daily analytical data set. Please see above for more detail on the relevant data collection.

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve?	Necessary or Discretionary?	Which benefit of the app does it support?
Exposure Windows See below for the full details of the Exposure Window date set Note: only relevant to GAEN Mode 2	Where a match between a Diagnosis Key and Contact is detected an Exposure Window is generated which captures the details used to determine if a app user is alerted. Never discloses the user that was matched.	Apple / Google EN API, when a contact match is made and an Exposure Window is generated [related to the event]	Aggregated on the Cloud platform to provide statistics	Generated on the App, shared with Cloud	Short. From match detection until aggregated into statistics	Statistics on matches being made are critical to understand and improve the performance of the contact matching configuration	Understand that matches are being made at expected levels. This allows us to understand the accuracy of the isolation advice. Foundation technology Relates to public health and the standard of service provided to the user.	Necessary	1, 6

Alongside these event analytical data sets, the following data items are captured.

Exposure Window Data Set

Data Item	Specific Use to support Exposure Windows
Local Authority (Area)	Please Note: subject to the re-identification protections for areas See Analytics Data Table above, Used to support the public health analysis of the data to understand differences across areas
Postcode District (Area)	Please Note: subject to the re-identification protections for areas See Analytics Data Table above, Used to support the public health analysis of the data to understand differences across areas
Phone Model	Enables the analysis of the data provided to account for and monitor the variations in phone model
Operating System	Enables the analysis of the data provided to account for and monitor the variations in operating systems
App Version	Enables the analysis of the data provided to account for and monitor the differences in the app version
Type of Event	Notes the type of event to support the accurate flow of data

See Table Analytics Data Table for information on why these data items are calculated

Exposure Window Data Set and Scan Instance Data Sub-set

The table below details the proposed data fields provided by the Exposure Window data set for analysis. The benefits, use and necessity of the data sets are noted above.

Exposure Windows

The following data items are captured when a shared Diagnosis Key is matched with a derived Broadcast code (noting the codification used to protect identity and privacy of individuals).

Data Item	Description
Exposure Windows: object	Used by GAEN Mode 2 and based on data recorded in the GAEN, when a broadcast code is received by an app user. The data object created when an encounter with an index case happens.
Exposure Windows: date	The relevant date of the exposure window
Exposure Windows: List of Scan Instances	Part of the Exposure Window object, contains technical data regarding the scanning that happens when two devices are in proximity, each window will contain multiple Scan Instances - this provides an approximation of proximity and duration of encounters

Data Item	Description
Exposure Windows: Risk score version	Reference note on which risk score calculation method was used. Allowing us to check the relevant risk algorithm that was used.
Exposure Windows: Infectiousness of Index Case (i.e. the app user who shared their Diagnosis Key)	Sharing of the Diagnosis Key, includes the ability the calculate the relevant date of symptoms onset and allows an infectiousness for the Diagnosis Key to be calculated. This helps calculate the risk score.
Exposure Windows: Risk Score	The risk score calculation from the measurements and risk basis
Exposure Window: isConsideredRisky	Validates whether the Exposure Window was equal or above the risk threshold for the app at the time it was generated.

Scan Instance

The Scan Instance is a data sub-set within the Exposure Window that captures the approximations of distance and duration used to calculate the risk of infection (risk score).

Data Item	Description
Scan Instances: min Attenuation	Minimum attenuation of the signal received during the scan (in dB) - will proxy as minimum distance for the encounter
Scan Instances: Typical attenuation	Typical attenuation of the signal received during the scan (in dB) - will proxy as average distance for the encounter
Scan Instances: Time since last scan	Seconds elapsed since the previous scan, typically used as a weight - will be used to understand the duration of the encounter

Test status and test process

The following data items are used to analyse the users test result and testing journey.

Data Item	Description
number of positive tests via Test Labs API	The number of positive test results (either 0 or 1) updated via the Test Lab API
number of positive test Token API	The number of positive test results updated via the user adding a test result code
number of negative tests Test Labs API	The number of negative test results updated via the Test Lab API
number of negative test Token API	The number of negative test results updated via the user adding a test result code

Data Item	Description
number of void tests Test Labs API	The number of void test results (either 0 or 1) updated via the Test Lab API
number of void test Token API	The number of void test results updated via the user adding a test result code

Isolation Status and Reason

The following data set is used to determine why the app user is self-isolating.

Data Item	Description
has Self Diagnosed Background Tick	Notes if the app is aware that the user has completed the questionnaire with symptoms; this currently happens during an isolation and for the 14 days after isolation.
has Tested Positive Background Tick	Notes if the app is aware that the user has completed the questionnaire with symptoms; this currently happens during an isolation and for the 14 days after isolation.
is Isolating For Self Diagnosed Background Tick	Notes if today the user is isolating because of answering the questionnaire (and has symptoms)
is Isolating For Tested Positive Background Tick	Notes if today the user is isolating because of a positive test result
is Isolating For Had Risky Contact Background Tick	Notes if today the user is isolating because of a risky contact

The following data item was reviewed as part of this update:

Data Item	Description
has Had Risky Contact Background Tick	Notes if the app is aware that the user has had a risky contact; this currently happens during an isolation and for the 14 days after isolation.

The following data items supporting this function are due to be collected shortly but are not included in the current releases:

Data Item	Description
Had A Risk Contact Notifcation Today	becomes 1 if user had a risky contact today, otherwise is 0 (Note this is impacted if the circuit breaker is in place)
started Isolation Today	Includes a count, i.e. 1, if the user started isolation today

Supporting Isolation Payments

The following data items are used if an app user seeks to apply for isolation payments.

Name	Description	Capture	Processing	Distribution	Lifespan	Benefit of processing
Isolation payments token	Single use temporary token generated to uniquely identify isolation period due to risky encounter	Generated in app back-end service	Stored in app and in app back-end. The gateway to verify that the transaction originated from the app and is valid for isolation payment	Passed between app back-end, app and gateway, and then passed to the The CTA Service (via ITS) for further processing of the claim	Up to the duration of the isolation period for contact cases (currently configured as 14 days from encounter date)	Used by the CTA Service system as part of two-factor authentication to ensure that application relates to a unique isolation period. For more details see the CTA Service system Privacy Notice and DPIA.
Encounter date	Date of encounter with index case for current isolation period that triggered the recommendation to isolate	Captured by app following exposure notification	Held in app until hand-off to gateway application process	Passed from app to app back-end and from app back-end to gateway	Up to the duration of the isolation period for contact cases (currently configured as 14 days from encounter date)	Used by the CTA Service to support eligibility checks for isolation payment.
Isolation end date	Date of end of current isolation period due to risky encounter with index case that triggered the recommendation to isolate	Calculated by app	Held in app until hand-off to gateway process	Passed from app to app back-end and from app back-end to gateway	Up to the duration of the isolation period for contact cases (currently configured as 14 days from encounter date)	Used by the CTA Service to support eligibility checks for isolation payment.

Future Analytical Requirements

For transparency future intention of analytical requirements is listed below. Please note that the features referenced are not yet in place and are not confirmed.

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve? (i.e. delivery of service, analysis, medical and public health)	Necessary or Discretionary?	Which benefit of the app does it support? 1: Get notified 2: check into venues 3: check your symptoms 4: Isolation Countdown 5: Medical Device Accreditation 6: Support public health & understanding of CV19
Symptomatic Questionnaire Answers Future functionality	Responses submitted in the symptomatic questionnaire. In particular the time between symptoms onset and filling in the questionnaire.	Captured within App as structured data capturing the questionnaire submission	Sent to the cloud with other stats, then aggregated in to summary statistics	Used to understand what % of users (and wider population) are reporting which Covid like symptoms	Aggregated in to summary statistics, which are then maintained as long as the app system is operational	Understand which symptoms are being reported, and how the symptoms are linked to the virology test results.	Public Health. Understand symptoms of users. Medical device requirement	Necessary	3, 5, 6
Opt-in Selections Future analytics for future functionality	If some features are optional to the users, which ones they select	Captured within App as text string	Sent to the cloud with other stats, then aggregated in to summary statistics	Used to understand what features users have opted-in to	Aggregated in to summary statistics, which are then maintained	Used to understand how many of the population are using particular app	Analysis. Understand what features users are using. Medical device requirement	Necessary	1,2,3,4,5, 6

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve? (i.e. delivery of service, analysis, medical and public health)	Necessary or Discretionary?	Which benefit of the app does it support? 1: Get notified 2: check into venues 3: check your symptoms 4: Isolation Countdown 5: Medical Device Accreditation 6: Support public health & understanding of CV19
					as long as the app system is operational	features, to gauge their popularity			
Contact Counts Future functionality	Counts of contacts with any other app users. Note: Not currently available on the GAEN.	Captured within App as integer contact count	Sent to the cloud with other stats, then aggregated in to summary statistics	Used to understand whether the app is detecting the number of contacts expected	Aggregated in to summary statistics, which are then maintained as long as the app system is operational	Enables refining the configuration of the GAEN to refine the level of contacts being detected, to improve performance on the app	Analysis. Understand that contacts are being made at expected levels. This will relate to the Personal Risk Score feature not yet available	Will be Discretionary	1, 6
Risk Accumulator Status Future functionality	The results of the apps risk analysis	Captured within App as structured data for a risk scored event	Sent to the cloud with other stats, then aggregated in to summary statistics	Used to characterise performance of the app risk scoring	Aggregated in to summary statistics, which are then maintained as long as	Enables risk scoring to be tuned and refined, to improve the performance of the app	Understand risk scoring. Information that is provided on what risky events have occurred. Foundation	Will become Necessary	1

Name	Description	Capture	Processing	Usage	Lifespan	Benefit of processing	Who needs the data item and what purpose does it serve? (i.e. delivery of service, analysis, medical and public health)	Necessary or Discretionary?	Which benefit of the app does it support? 1: Get notified 2: check into venues 3: check your symptoms 4: Isolation Countdown 5: Medical Device Accreditation 6: Support public health & understanding of CV19
					the app system is operational		technology		
Risk API Decisions Future functionality	Decisions made by the Risk API Circuit Breaker	Captured within the Risk API cloud service when asked to make a decision	Aggregated in to summary statistics	Used to characterise performance of the app risk scoring and decisions	Aggregated in to summary statistics, which are then maintained as long as the app system is operational	Enables risk scoring to be tuned and refined, to improve the performance of the app	Understand risk scoring. This is the decision that is subsequently made based on the risk event (risk accumulator status). Foundation technology	Will become Necessary	1

Appendix 2 – APIs presented by Cloud Services

COVID proximity app – operational stages and system flows

- Analytics – Collects analytical data from the app for aggregation and statistical analysis (stateless)
- Analytics – same API used for Event Analytical Data Set – Collects analytical data from the app for aggregation and statistical analysis (stateless)
- Config – Provides configuration for the app, possibly based on device state like language and type (stateless)
- Distribute – Access the data used for risk scoring; positive diagnosis keys, hotspot QR codes and postcode district/local authority risk levels (stateless)
- Risk – Confirm with the cloud services before taking a risk based action such as isolation (conversational – The App request is returned a short-lived transaction Id, which the app uses to check to see when the decision is made. Token is likely to be needed for up to 4 hours.)
- Submit – Submit Exposure Diagnosis keys to be added to the positive key set (stateless)
- Control – Support the Control Panel web monitor (stateless)
- Swab testing – App-facing API used to get a Transaction Token and get the Swab test results (conversational – a transaction ID token is maintained while a Swab test is underway, which is expected to be 1 to 4 days)
- TestLab – 3rd party Test Lab API used by the Swab test Labs to submit Test Results, together with the linking Token ID (conversational – a transaction ID token is maintained while a Swab test is underway, which is expected to be 1 to 4 days)
- App Rest API client – collects and provides data to support operational interoperability with partner Health Service apps (stateless)
- Supporting Isolation Payment Application APIs (please note: this may differ for Wales)
- TTSP Gateway API – supports the user's application in accordance with the app's privacy requirements (stateless)
- TTSP Mobile AP – creates and updates the token for the app user making an application (conversational, the transaction of tokens is confirmed)

Appendix 3: data flows

Inflows

Sender	Content	Pseudonymised?	Mode	Security	Recipient
User – installed App	Diagnosis Keys	No - not identifiable	Submit API	-	DHSC secure computing infrastructure
User – Installed App	Daily Analytics	Anonymous	Analytics API	-	-
User – Installed App	Event Analytical Data Set	Anonymous	Analytics API	-	DHSC secure computing infrastructure
National Pathology Exchange (NPEx)	When test results are received from a lab, NPEx matches result to ref code and sends the code, result and test date to DHSC secure computing infrastructure.	Yes	CSV file	Security: TLS with API key, IP source address restriction	DHSC secure computing infrastructure
Federated Servers	Diagnosis Keys	Anonymous	App Rest API	-	DHSC secure computing infrastructure

Outflows

Sender	Content	Pseudonymised	Mode	Security	Recipient
DHSC secure computing infrastructure	Diagnosis Keys submitted by COVID-19 positive users	No - not identifiable	Distribute API	-	User / Local Application
DHSC secure computing infrastructure	Diagnosis Keys submitted by COVID-19	No - not identifiable	Distribute API	-	User / Local Application

Sender	Content	Pseudonymised	Mode	Security	Recipient
	positive users				
DHSC secure computing infrastructure	Diagnosis Keys	No - not identifiable	App Rest API	-	Federated Servers (under control of Scottish programme)
DHSC secure computing infrastructure	Isolation Support Payment token and supporting data	No - not identifiable	TTSP Gateway API		
TTSP Mobile API	-	DHSC secure computing infrastructure			

For a full list of recipients of Diagnosis Keys shared with the Federated Servers see the section on interoperability

Appendix 4: Guidance for completing a risk register

All risks need to be assigned a likelihood and impact score. The likelihood and impact scores will be calculated and used to understand the level of severity/importance:

Likelihood scores

Likelihood score	Descriptor	Frequency – how often might it happen?
1	Rare	This probably will never happen
2	Unlikely	Do not expect it to happen/reoccur, but it is possible it may do so
3	Possible	Might happen or reoccur occasionally
4	Likely	Almost certain to occur, but it's not a persisting issue or circumstance
5	Most certainly	Almost certain to happen/occur; possibly frequently

Impact scores

Likelihood score	Descriptor	Frequency – how often might it happen?
1	Very low	Unlikely to have any impact
2	Low	May have impact
3	Medium	Likely to have an impact
4	High	Highly probably it will have a significant impact
5	Very high	Will have a major impact

Using a Red, Amber and Green (RAG) system for scoring risks means they can be ranked such that the most severe are addressed first. Decisions to prioritise risks can be made using the RAG rating and mitigating actions put in place to alleviate the risk.

Impact						
	Very High -5	A	A/R	R	R	R
	High - 4	A	A	A/R	R	R
	Medium - 3	A/G	A	A	A/R	A/R
	Low - 2	G	A/G	A/G	A	A
	Very Low - 1	G	G	G	G	G
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
		Likelihood				

"RAG" rating system

Appendix 5: anonymisation of analytical data collected

The NHS COVID-19 app ("the app") collects analytical data to ensure the app is working properly, safely and helping manage the COVID-19 public health emergency. The methodology and protections that anonymise app users are determined by the Apple/Google API and non-identification of users is a condition for using their contact tracing functionality.

You can read a summary of this appendix.

Data and the app

Your app retains data within the app around specific interactions. The logs of who you have interacted with are retained within the Apple/Google GAEN and are not visible or accessible to us. Details of which venues you have visited again are only on your app. The app will hold details of a relevant test result but only for as long as necessary, 14 days after any self-isolation period this data is no longer recorded. As detailed below you can delete the app, or just some data items (specific venues) or all the data it contains.

Data provided to the app by the central systems

The central system provides all app users with three key sets of data. Every app user receives the same information, called reference material, which the app uses to determine if you need to receive an alert or advice. These are:

- the list of Diagnosis Keys from app users who have tested positive. This functionality keeps the identity of app users anonymous to other app users;
- the list of all postcode districts, which are mapped to local authorities, and their current risk level
- the list of venues that could pose a risk, as determined by the Venue alert process

Systems also provide you with an update to your status if you used a test code provided through the app.

Analytical data

Each day, the app collects a summary count of key information. This is called the analytical data set and helps us monitor the use, performance and information about the app and its use. The data is prepared and will be sent to central systems where it used for assurance of the app, technical checks and the public health functions. It does not include the data held on your app about specific venues or your close contacts.

Event Analytical data set

The Exposure Window data sets are a new type of data set collection for the NHS COVID-19 app. With the introduction of updated functionality from Apple and Google, the GAEN Mode 2, new data items are available to support the alert notification process, the analysis of alerts and knowledge about the public health emergency.

Access control, audit logs and oversight

Our safeguards ensure only people who are authorised and need access as part of their role will have access to the analytical data. For example, no user can remove data from our technical environments and where even negligible risks of identification are considered safeguards such as small number suppression are brought in.

All flows and use of data are under strict control and testing. The National Cyber Security Centre and other key cyber security experts continue to advise and recommend on how to protect and preserve the privacy of app users, including the controls and techniques we use to anonymise and aggregate data.

To further support the privacy of app users, we have put in place organisational safeguards to ensure separation between all technical data that is used to check the app is working and the analytical data can only be used for approved public health purposes.

With these controls, monitoring and safeguards in place we conclude that the risk to data privacy of an app user being identified by a combination of factors (e.g. phone model and operating system, plus postcode district), would be negligible to non-existent.

We use small number suppression in the performance view and dashboards. Any query or result that would result in a number below 5 is suppressed. For example, the following data items are the most likely to trigger small number suppression when combined with other data items in a query: onboarded users, users isolating due to risky contact and/or users' isolation, users completing questionnaires, tests recommended and user check in counts.

User data journeys

In order to explain how app users' data is generated and collected we have laid out a number of different scenarios about using this app. These are our User Data Journeys where we set out what data is generated, where it is held and where it flows. We reference the data that flows to app users and what category of data (for example, aggregated or anonymous) they fall into.

The User Data Journeys included below are:

- Overview for all App Users

- Interaction with Index Case
- Venue Check-In Users
- App users who only use the contact tracing within the app
- App users who use all the functionality of the app
- App users booking and receiving test results via the app

Definitions

The following definitions are used within the DPIA, Privacy Notice and for this document.

Term	Definitions
Aggregate	Aggregated data: Combined data from one or more data sources, potentially including summated or summary data or information or statistics based upon living natural persons' data sourced from or related to one or more individuals to show general trends or values or analyses without identifying individual personal information or data within the data set.
Anonymised	Anonymisation: The process of rendering data into a form which does not identify individual living natural persons or makes the risk of re-identification sufficiently low in a particular context that it does not constitute personal data.
Anonymous	Data that cannot identify a living natural person.
Data minimisation	this is the minimum data to deliver the functionality as designed and necessary to the purpose.
De-personalised	De-personalised data: This is information that does not identify a living natural person, because all relevant identifiers or identifiable data have been scrambled or removed from the non-identifiable information about the living natural person to whom it relates. Because the information relates directly to a living natural person it must be protected in law. It might, in theory, be possible to re-identify the individual if the data was not adequately protected, for example if it was combined with different sources of information.
De-identified:	This refers to personal confidential data relating to a living natural person, which has been through anonymisation in a manner conforming to the ICO Anonymisation code of practice. There are two categories of de-identified data: 1. De-identified data for limited access: this is deemed to have a high risk of re-identification if published, but a low risk if held in an accredited safe haven such as an approved secure operational data store and subject to contractual protection to prevent re-identification; 2. Anonymised data for publication: this is deemed to have a low risk of re-

Term	Definitions
	identification, enabling publication.
Index Case	Within the context of the app, an index case is an app user who has tested positive for COVID-19: Updated their status within the app; Chosen to share their Diagnosis Keys Sharing these Diagnosis Keys allows other app users to be alerted by their app when appropriate. This is done by calculating the risk of infection from the two app users interaction.
Linked data	Linked data: The result of merging data from two or more sources with the object of consolidating facts, potentially including those relating to a living natural person, or an event that are not available in any separate record.
Personal	Personally identifiable data: This term describes personal information about identified or identifiable living natural persons, which should be kept private or secret. It includes the definition of personal data in the Data Protection Act, but may also include data relating to people who have died and information given in confidence under the Duty of Confidentiality. It includes, for example, Personally Identifiable Information (PII) and Sensitive Personal Information (SPI).
Personal Confidential Data (PCD):	Personal Confidential Data (PCD): Personal information about identified or identifiable living natural persons, which should be kept private or secret. For the purposes of this Review 'Personal' includes the DPA definition of personal data, but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive' as defined in the Data Protection Act.
Personal Data	Personal data: Data which relate to a living natural person who can be identified from those data, or from those data and other information which are in the possession of, or are likely to come into the possession of, the data controller, and includes any expression of opinion about the living natural person and any indication of the intentions of the data controller or any other person in respect of the individual.
Pseudonym	Pseudonym: Individuals distinguished in a data set by a unique identifier which does not reveal their 'real world' identity.
Pseudonymised	Pseudonymisation: The process of distinguishing living natural persons in a data set by using a unique identifier, which does not reveal their 'real world' identity (see also Anonymisation and De-personalised data).
Pseudonymised (as defined in GDPR)	In GDPR (Article 4) 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of

Term	Definitions
	additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable living natural person.

Definitions are based on the National Data Guardian for Health and Care Review of Data Security, Consent and OptOuts and Connected Health Citites Data Glossary

Context

You generate data through your use of the app. Specific functions will generate different data items. For example, venue check-ins will add details of the venue onto your app. The analytical data set collected about your venue check-ins is the number of venues checked into and the number of failed or cancelled venue check-ins. No other details about the venue are collected or available to the analytical data set.

This count allows us to monitor how well the app is working and which functions are being used. We can monitor how well the app is working whilst preserving the privacy and identity of app users.

The analytical data set collected from the app prevents it from being linked to other data sets held by us, the Department of Health and Social Care, as data controller. See below for the specific example of test results and the app.

Other Test and Trace Services

Contact Tracing

As an app user, you may be contacted by national or local contact tracers. Your details will have been provided by other members of the public who believe they may be at risk or may pose a risk of COVID-19 infection to you. This does not relate to your use of the app and no details exist within the app that could be passed to contact tracers. However, if helpful you could use your app to help you provide details of the venues you checked into to the contact tracers. They, and we, have no access to that specific information.

Testing

The process of ordering and returning a test results protects the user's identity and privacy through several techniques. These include minimising data flows, ensuring that only necessary systems have access to the data needed for their part of the process.

If you use a code generated through the app to book and test, your status will be sent back to the app. When you book the test, the only details that are passed to the website is the test code provided via the app. The details you enter into the website when booking a test,

which includes personal data, are not available to the app and cannot be linked to the analytical data set generated by the app.

Co-ordination between services ensures the correct test result gets back to you and to your app. However, we separate out the codes and use tokens to ensure that the data cannot be linked. Once the result is returned to you via the app, the test code is deleted from our systems.

New functionality for national launch will allow anyone receiving a test (in England and Wales) to enter a code provided during testing to update the app with their test result and status. This is available to support those using the app who did not generate a code (i.e. they booked their test independently from the app).

Venue Check-Ins

Currently, venue check-ins details are updated from central systems but no details about who or how many users attended a venue is recorded. Local Health Protection Teams (HPTs), national Public Health Experts and the Joint Biosecurity Centre work together to help determine what venues should be considered at risk. This decision not only relates to updates for app users but for local HPTs and services.

Isolation Support Payment

Recent updates for the app support an app user in applying for isolation support payments. When recommended to self-isolate due to a contact with a risk of infection, in England the app user can apply for the isolation payment. Support for this process is expected in Wales shortly.

Data Sets

The Analytical Data Set differs between Apple and Google (Android) to account for differences in the functionality.

The following data is collected from Apple app users but not from Google (Android) users:

- Cumulative Cellular Download Bytes (Data to app by cellular)
- Cumulative Cellular Upload Bytes (Data from app by cellular)
- Cumulative Wifi Download Bytes (Data to app by wifi
- Cumulative Wifi Upload Bytes (Data from app by wifi)

This data relates to the app’s receipt and transmission of data across different types on network.

App data environments

The app holds data in the following 3 environments:

1) App

The app holds data generated by the app, and when prompted can request access to the diagnosis key provided by the Apple Google functionality (the GAEN). The contacts held by this function cannot be viewed by the app and the DHSC.

The app holds data about the user (the venue's they've checked in for example) as well as reference material provided to all app users to support the functionality of the app (for venue check-ins the details of venue's that may pose a risk to of COVID-19 infection).

The app holds:

the data held on the app (Personal Data to you, but not accessible to us)

the analytical data set (prior to it being submitted) which we protect to make anonymous once it leaves your app.

2) Product

This is the central system that supports the app and its users. It manages the APIs that deliver information to and from your app. The data within the analytical data set arrives within this environment and is managed by the software and systems it contains. This environment also sends out the updates to all app users. Performance View – dashboards to help oversee the service delivered to app users

3) Analytical

Subject to additional controls, the analytical data set is provided to data scientists within an analytical environment to monitor, improve and evaluate:

- the app,
- our understanding of COVID-19
- the Public Health response

Understanding the Data Flows

This table sets out the data flows, how and when they are triggered.

Functions of the App	Data Held on the App	Analytical Data Set and Event Analytical Data Set	Data Flow to the Product Environment	Data Flows from the Product Environment	Product Environment (via APIs)
As you interact with the different functions of the app, you will generate data. Some within just the Apple/Google functionality, and some within our app. Those interactions, detailed below, are captured in the analytical data set. These logs do not detail individual events but counts or summaries of which functions are used.	Data held on the app falls into the following categories Data about the user: Details about a relevant test status, venues checked into, the postcode district and the contact detected. Reference material: The app will hold data about each postcode districts level of risk and “at risk venues”. This allows the app to appropriately update the app user. It will also hold a list of the Diagnosis Keys that could pose a risk to	As you interact with different functions, the analytical data set on the phone is updated. For example, if you check into a venue this adds one to the count of check-ins. If this fails, is abandoned or cancelled then another count is updated. As discussed above, this helps us determine if the app and its functions are working properly.	Each day your app will bundle its current analytical data and provide it to the central system’s API (how the system and app communicates). Whilst the timing is set by the app it is dependent on access to the network and systems.	On average at 2 hour intervals, the product environment (central system) delivers updates to all app users on app users who have tested positive (via the Diagnosis Key), “at risk” venues and the risk of postal venues.	As the analytical data set lands, it is treated (for example, the IP address is removed) and added to the data store. No user ID is sent from the app with the analytical data and any ID assigned on landing is not consistent across analytical periods. (For example, the row level for the same user will likely never be the same across uploads). This helps ensure we cannot identity which app user is you.

Functions of the App	Data Held on the App	Analytical Data Set and Event Analytical Data Set	Data Flow to the Product Environment	Data Flows from the Product Environment	Product Environment (via APIs)
	app users. These alert app users without the app sharing the identity of those app users.				

Updating the app and app users

The app is updated by the central systems (product environment), on average, every 2 hours. This will include an updated list of diagnosis keys (from app users who have tested positive), of venues that may pose a risk and the latest area risk status. This data triggers the app's functionality for relevant users. For example, if you checked into a venue during a relevant period and may be at risk – you will receive a notification.

Where an app user has tested positive for COVID-19 they will be prompted to share their protected ID. Once these are processed by the central system, they are provided to all app users. The Apple Google functionality uses these codes to determine if you should be alerted. This is distinct for the NHS COVID-19 app.

Once the data is provided to the app user, the app checks whether any alerts or notifications need to be displayed to you. This is based on how the app works, is supported by automated decision making and uses the reference material provided to all app users.

Data generated and collected

This section sets out different aspects of the data why it is generated or collected and what function the data serves.

Apple Google GAEN

Your app will hold the following, subject to the controls of the Apple Google Functionality and provided via the Exposure Notification API.

The app holds the broadcast codes from other app users you have been in contact with, including the details that allow the app to determine whether you might be at risk

These broadcast codes are changed every 15 minutes and are not accessible to you as an app user or us as data controller.

This system is designed by Apple and Google to protect the privacy and identity of app users, making their use of the app anonymous.

As part of the routine update the app receives details of all Diagnosis Keys that could pose a risk, another set of reference material used by all app users. The app's functionality combined with Apple Google GAEN help determine if any of the broadcast codes should trigger an alert for the app user. They do this by determining is broadcast code relates to a diagnosis key through a process that maintains the privacy of both parties.

With the introduction of GAEN Mode 2, the Exposure Window data set is used as part of the risk algorithm and risk score calculation process. The data sets are also sent to the DHSC secure computing infrastructure as a Event Analytical Data set.

Data Held on the App

Beyond the digital contact tracing all app users will have the details listed below on their app. The same reference material is on everyone's app. Other details will vary with how you use the app but are only held on your phone.

The App

The app will retain your declared postcode district, selected local authority, latest virology test result and any venues visited. This data can be deleted when you delete the app, through the app and even for individual venues. No history of postcode districts, local authority or virology test results are retained.

Data about the user

QR Venues Visited (details of the venues checked into)

Postcode District (the users current declared postcode district)

Local authority (the local authority selected by the user after they input their postcode district)

Virology Test Results (the last test result retained for the isolation period plus 14 days)

Reference Material (used to appropriately update the app user)

In addition, to the diagnosis key detailed above, the app holds two sets of reference material which enable the app to function and appropriately update you. For example, the list of risk status for postcode district, within a local authority, allows you to be notified about any changes to the risk score as well as display the baseline risk.

Risk status for every postcode district/local authority within the app [Area Risks]

Full list of venues that are "at risk" with details of the relevant time period [Hotspot QR Venues]

Analytical Data Set

Using the app will populate the analytical data set. As noted above, the majority are summaries or counts of function use and do not list data items.

This data is not only important to understanding if the app is working as expected, to manage the transmission of COVID-19, but it also supports us in meeting our statutory obligations to app users.

For example, our obligations include equalities and health inequalities. Monitoring the data, storage and use of the pause function allows us to understand the potential impacts of the app and its use. This helps to ensure that the app supports as many communities and users as possible. For example, if the app uses large amount of data then those on limited data plans may not be getting the service we want to provide.

All users potentially generate the following data items in the Analytical Data Set.

Core details

The app collects the following details about your phone, the app and the analytical period the data applies to:

- Start Date – when the period for the analytical data began
- End Date – when the period for the analytical data ended
- Postcode District – the current postcode district of the user
- Device Model – the device model
- Operating System Version – the operating system in use on the phone
- Latest Application Version – the application version of the app

Data Usage of the app and data submitted to the app

The data usage of the app on your phone. This helps us to monitor how much data the app is using and whether this in line with expectations.

- Cumulative Download Bytes (Data to App)
- Cumulative Upload Bytes (Data from App)
- Cumulative Cellular Download Bytes (Data to app by cellular)
- Cumulative Cellular Upload Bytes (Data from app by cellular)
- Cumulative Wifi Download Bytes (Data to app by wifi
- Cumulative Wifi Upload Bytes (Data from app by wifi)

Service and system checks

These data items are used to ensure the service and system is working correctly.

- total Background Tasks
- running Normally Background Tick
- completed Onboarding – whether the app user has completed the onboarding process and the app requirements assessment as a “in use”
- includesMultipleApplicationVersions – a check that only one of version of the app is in use.

See below for an overview what background tasks are and this data set.

Function specific data in the analytical data set

The following data items are present for all users but vary by the functions you use. Where not used your data return will be zero (or nil) for the relevant entry.

Venue Check-In

- Checked In (count of venue check ins)
- Canceled CheckIn (count of venue check ins cancelled - not check outs)

Test Results and Reason (into the app)

- number of positive tests via Test Labs API
- number of positive test Token API
- number of negative tests Test Labs API
- number of negative test Token API
- number of void tests Test Labs API
- number of void test Token API

Pause functionality

- Encounter Detection Paused Background Tick – allows us to judge how the long the app was paused for

Symptom Checker Use and Results

- Completed Questionnaire And Started Isolation- when the symptom checker was used and recommended a test and self-isolation;
- Completed Questionnaire But Did Not Start Isolation - when you used the symptom checker but self-isolation wasn't started regardless of result

Isolation Trigger

The following provide an overview of whether an app user is isolating and for how long. It cannot be used for any enforcement.

- has Had Risky Contact Background Tick
- has Self Diagnosed Background Tick
- has Tested Positive Background Tick
- is Isolating For Self Diagnosed Background Tick
- is Isolating For Tested Positive Background Tick
- is Isolating For Had Risky Contact Background Tick
- is Isolating Background Tick

Analytical Data upon arrival at the central system

No identifiers are provided to the data as it leaves the app, preventing you from being identified across analytical data packets (subject to additional controls). On landing data will be placed into a row.

- Row Level

Background tasks

In line with most apps, the NHS COVID-19 app uses "background tasks" as a way for the app to keep content up to data and for the app to function in the background of your phone. For example, when you are using another app or have the app minimised. These background tasks are normal functions of your app interacting with your phone's operating system.

Background tasks do not enable us to track the location of users, or to read any other information from the phone for example about other apps and how you use them.

Every time the app interacts with the operating system it creates a “background tick” which helps us to understand how often certain app functions might be being used and if the app is working as expected. Typically, we would expect to see the app interact with your phone’s operating system up to 12 times, and a minimum of 0. If 0, this implies that the app was not running that day.

We use this count from background tasks as a comparator to:

- see how many active users the app had fully operational on a given day;
- Diagnostics - to ensure that the app was running correctly, as certain metrics should be no higher than the background tick (e.g. a user is self-isolating);
- Number of times encounter detection was triggered.

This data is used as a count or summary and not with any identifiers from the user. This makes sure that we don’t know which app user they apply to but allows us to understand how the app is being used and if it is working effectively.

Protecting your privacy and identity

The following summaries outline the key techniques we use to protect every app user’s privacy and identity, as well as our analysis of the risks from particular data items. We try to make sure that an app user can use the app anonymously whenever possible, with the minimum data collected that is necessary to deliver the functions of the app. However, the data collected must provide an effective service to app users and help us understand and manage the COVID-19 public health emergency.

We have included a review of the risks and protections for each environment within our Data Protection Impact Assessment.

Personal Identification Risk

The analytics data relating to app operation is collected as summary counts, for example the number of exposure events and QR code check-ins. The details of specific exposure events and QR code check-ins never leave the mobile device on which the app is running. We cannot access any information on your specific contacts or location check-ins.

Anonymisation Strategy: Technical data items

The analytics data is collected and held in such a way that it cannot be used to identify the user. Firstly, no data is collected which would allow us directly to identify an individual – we do not collect details of the user’s name, address, phone number, device IMEI or any other unique piece of identification. Secondly, the data that we do collect is held so it cannot be put together (“linked”) to identify a user – specifically, we separate all technical data

relating to the phone, used to ensure the app is functioning properly, from the public health data that we need to manage the pandemic.

This is done by using different environments to manage the data with additional controls around the public health data and broader analytical functions.

The technical tech items are detailed below along with the risks of identification that could arise.

Phone model and operating system

The app supports as many phone models and operating systems as possible. This data is used to check that the app is working properly. With a version of the app available to the population of England and Wales there should be enough app users to prevent the identification of any single user from the uniqueness of their phone make, model and operating system.

If an app user happens to have a very unusual phone model and operating system, it may be possible that they will be the only person in their postcode district with that combination of phone model and operating system. However, unless an app user made their phone make, model and postcode district publicly known, we could not possibly identify them from this data set. To further mitigate this risk, we have taken steps to ensure we cannot identify how many phones of a particular model and/or operating system exist within a given postcode. Removing this link should make it impossible to identify a given user by reference to their phone.

App Version Number

The app version number helps determine how many app users are using the current version of the app. There are likely to be a small number of version releases of the app, with each version downloaded by a large number of users. Our analysis has not found any situation where only one individual is using a particular version of the app and could be potentially identifiable as a result.

Onboarding Status

The onboarding status of an app on a user’s phone is binary – either “complete” or “not complete”. On the assumption that a large number of users will be using the app and represented in each of these categories at any one time, our analysis shows that a specific user could not be identified from this information.

Usage, storage and data download usage

We do not see any situation in which the data we collect about usage status (i.e. whether the app is updating correctly), storage usage on a phone and data download usage on the

phone would allow us to identify an individual app user as this is unlikely to be unique to any identifiable person.

This analytical data set does include the user's phone model and operating system which tend to relate to the usage and storage statistics. This would not add any addition risk of identification beyond those associated with unique phone model and operating system combinations.

IP Addresses (Not used by the app)

Your IP address (a unique identifier for your phone when you use the internet) is automatically shared with the Department for Health and Social Care (DHSC) when you share data through the App. DHSC does not use your IP address however and deletes it as soon as it is received. Like every other app, our app uses the internet to work which requires the use of the IP address.

The application is reviewed and tested to make sure that there never exists functionality that collects, logs, retransmits or stores the IP addresses received within HTTP headers. This minimises the possibility of recombining IP address and payload data.

We have no intention of collecting IP addresses to attempt to identify app users and have these technical safeguards to remove any possibility of this being attempted. Protecting the identity of users, and demonstrating those protections, is a core condition of the use of the Apple/Google Contact Tracing functionality.

Anonymisation Strategy: Public Health data items

The same anonymisation, data minimisation and tests to ensure the items are necessary are used with data items that are used either solely for public health or for both functions. A key requirement is to protect the identity and privacy of you as an app user.

Postcode District

The postcode district entered by the user is potentially identifiable data. Most postcode districts have around 8,000 households in them and we expect a large number of users to download the app within each postcode district. Our analysis suggests that is a negligible risk of an app user being identified at postcode district level.

We have accounted for the postcode districts with smaller population densities (e.g. less than a thousand) by grouping these smaller postcode districts with other postcode districts to ensure the group represents at least 8,000 households. Postcode districts in incoming analytics messages are changed to this group identifier before persistence (i.e. before being stored and made available for analysis). As detailed above, any reporting also considers the need for small number suppression.

Where postcode districts could be combined with other data items, for example test results, that might indicate a small number of app users, we add further protections. These include techniques such as small number suppression and the removal of these data items for non-technical analysis.

Alongside the additional controls to prevent linkage and holding the app data as distinct data sets, this prevents you as an app user being identified through the data we hold about your use of the app.

The user's area, both local authority and postcode district, is stored on the app. The user's local authority and postcode district will take account of interactions that result in fewer than 1,000 households to minimise the chance of re-identification.

The Local Authority is collected as part of the analytical data set and is subject to the same standards and controls to remove the risk of re-identification.

Quantity of Exposure Events and QR Code Check-in Counts

We do not collect any information which would allow us to identify which app users have been in contact with each other user, or the venues they have checked in. The decentralised app system we have adopted achieves this, by ensuring this information is only held on users' phones.

Our review of the risks demonstrates that recording the overall number (quantity) of exposure events and check ins does not present any risk of users being identified as we do not link this information to individual users. For example, the information that a person had checked in to (say) five venues or had ten proximate contacts, would not allow us or others to identify them. We do not identify which venues and do not associate that information with any other details (for example, postcode districts).

Venues/Business can register for an official NHS QR code. As the venue check in is only held on the phone, with just a count being taken of venues, we would be unable to determine whether 1 or 300 people had "checked-in" to any venue either routinely or even when issuing an alert for that venue.

Pause Usage

When we collect information about how long contact tracing has been turned off on the app, we do not link this to individual users or other information that would allow us to identify a specific user. If a user wants to turn, contact tracing off altogether they also have the option to delete the app.

Symptomatic Questionnaire Results and Isolation Status

We collect a simple "yes" or "no" to whether the app advised a user to isolate and seek a test. We do not collect information about individual users' symptoms beyond whether they

might or are not indicative of COVID-19. Nor do we collect data as to how much longer a user has left to isolate, only that they were isolating at the moment the data was collected.

Swab Test Results

If an app user has linked their test result to their app, we take data as to whether or not the test was positive in order to compare the actual test result against what we advised the user to do, to monitor and improve how the app works.

When the app is used to provided test results back to the user, the data is promptly deleted, and the techniques across the data flow involves compartmentalising the data and codes to prevent any reidentification of app users from these details.

The name and address information used to book an actual test is not passed to the app, and there is no way of identifying that an identifiable person has tested positive via the app. Also, this data is not linked to other data which could in combination identify the individual user (e.g. the postcode district, model or operating system details of their phone).

Risks of Identification outside of the App

Small numbers of contacts.

While it is unlikely ever to happen, our privacy notice makes users aware that there are some unusual circumstances in which another person might be able to identify that they were the person who had tested positive when they receive an alert.

For example, if an App user had only been in contact with a single person and no one else, they would be able to infer who the infected person was when they received an alert (i.e. the only person with whom they had been in contact). This risk could also happen with manual contact tracing.

We have noted the privacy risk in our risk register but recognise that this is an underlying risk in the context of contagious diseases and public health management.

User choices

Deleting the app

Should you wish to cease providing analytical data they have the option to delete the app from your phone at any time. Safeguards to prevent the identification of you are so robust that we would not be able to determine who that user was in order to delete or remove any analytical data they had already submitted.

Deleting data held by the app

You can choose to delete all of the data held by the app or just individual venues that you have checked into. This will stop you receiving any alerts from the app based on the information you have deleted. It will not be present for the app to check against the lists provided by the central system.

If you choose to delete the postcode district in the app, this will also delete venue and other details. It acts as a reset for the app.

The data about your use of the app will still be in the analytical data set and these summary counts will be submitted for the relevant period and will continue to be unless you delete the app.

Digital Contact Tracing (Exposure Window, Exposure Logging and Exposure Notification)

The methodology and protections that maintain the anonymity of app users through contact tracing are determined by Apple and Google. The functionality and Exposure Notification API (GAEN) that provides this service has strict conditions of access and use, which the NHS COVID-19 app uses. For both contact tracing functionality and any analysis delivered by the app – non-identification of users is a condition of access for Apple and Google. We are happy to comply with that standard.

The User Data Journey

These scenarios provide examples of the data generated and collected when you use the app. We have included the most relevant ways we protect your identity and privacy, through anonymising and aggregating data along with other safeguards.

Scenario: All App Users

We have detailed above the data generated and collected by the app, along with what it is used for. For this example, we've repeated some of that information, so you can see how this works in practice. This scenario is updated to reflect the latest changes to the app. See section on recent updates to the app for more information.

For all users who complete onboarding and are using the app, key information will be collected in the app and as part of the analytical data set. Data will be held within:

- the Apple Google functionality (the contact tracing) until a request to share that is triggered by a positive test result;
- within the app (and will always be retained only within the app);

- as part of the analytical data set which will remain on the app until the app triggers the upload to the APIs that interact will the central system.

In addition, the digital contact tracing functionality provided by Apple and Google (the Google Apple Exposure Notification or GAEN) now includes:

- Exposure Window data collect and data set.

The Exposure Window data set is triggered when your app registers that a shared Diagnosis Key, provided by another app user, can be derived from a broadcast key held on your phone. This is registering a close contact and potential risk of infection on your app.

The data set allows the app to:

- Calculate your risk of COVID-19 infection;

- Where appropriate give an alert and advice (i.e. that you are at risk and should self-isolate)

The Exposure Window(s) for each 30 minutes of contact are provided as part of the analytical data required by the app. They are held on the app until the app triggers an upload to the APIs that interact with the central system

Digital Contact Tracing

Digital Contact Tracing

The Apple Google functionality generates a daily code for the app user, a broadcast key (changed every 15 minutes) is passed to other app users who are in contact (via Low Energy Bluetooth or “BLE”). An app user who tests positive for COVID-19 and who chooses to share their codes (protected as diagnosis keys) has this code added to the list of “potential risk” users provided to all app users.

Each individual user’s app will check whether they have a broadcast key associated with a diagnosis key on their phone. If a derived (i.e. a broadcast code produced from the diagnosis key) code is present and meets the set criteria – the app will alert the user. This functionality and the identity protection within this process are provided by Apple Google. However, the NHS app sets the criteria for when an alert should be issued.

Our working with health services in Gibraltar, Jersey, Northern Ireland and Scotland allows app users across all of the digital contact tracing apps to support this functionality. By giving permission to share diagnosis keys, app users in England and Wales can make sure that other app users receive alerts when appropriate. This is regardless of which digital contact tracing app they use or which jurisdiction they are in.

Apple Google GAEN Mode 1

This is only relevant for app users who have not updated their NHS COVID-19 app. It is strongly recommended that users routinely update their app in order to get the most effective service.

A user's app will hold, subject to the controls of the Apple Google Functionality and provided via the Exposure Notification API.

- The broadcast keys from other app users they have been in contact with, including the details that allow the app to determine whether the user might be at risk;
- These details include a measure of distance and duration of contact.

This enables that routine checking of whether an app user needs to be alerted of a potential COVID-19 risk from another app user. You won't know which user from the details the app provides and we, the DHSC, cannot identify either you or the app user who generated your alert.

Apple Google GAEN Mode 2

The new version of the Exposure Notification functionality (GAEN Mode 2) adds a layer of detail to the previous version (GAEN Mode 1), this uses the Exposure Window data sets and events to calculate the risk.

Much like GAEN Mode 1, a user's app will hold subject to the controls of the Apple Google Functionality and provided via the Exposure Notification API.

- The broadcast keys from other app users they have been in contact with, including the details that allow the app to determine whether the user might be at risk;
- These details include a measure of distance and duration of contact.
- This enables that routine checking of whether an app user needs to be alerted of a potential COVID-19 risk from another app user. You won't know which user from the details the app provides and we, the DHSC, cannot identify either you or the app user who generated your alert.

In addition, the GAEN Mode 2 captures 30-minutes Exposure Windows for interactions between the app user and index cases (see above for the definition) who have shared their Diagnosis Key and may pose a risk of infection. Within each Exposure Window is a Scan Instance which captures the approximate duration between the contacts and distance between.

With Mode 2 of the GAEN app, the Exposure Windows for any contacts are submitted to the Analytical API for use in the Analytical Environment.

Data Held on the App

Outside of the digital contact tracing, all app users will have the details listed below on their app. The same reference material is on every user's app.

Other, non-reference, details vary with how you use the app but are only held on your phone.

The App

The app will retain the user's declared postcode district, the selected Local Authority (from those suggested by the users postcode district), latest virology test result and any venues visited. This data can be deleted when you delete the app, through the app and even for individual venues. No history of postcode districts or virology test results are retained.

Data about the user:

- QR Venues Visited - details of the venues checked into;
- Postcode District - the users current declared postcode district;
- Local Authority – the local authority selected by the user (based on their postcode district);
- Virology Test Results - the last test result retained for the isolation period plus 14 days;

Reference Material (used to appropriately update the app user):

The app holds two sets of reference material which enable the app to function and appropriately update the user. For example, the list of risk status for postcode district allows the user to be notified about any changes to the risk score for their postcode district as well as display the baseline risk.

- Risk status for every postcode district within the app (Area Risks)

The Risk Status, or Tier, for area will be set by the Local Authority though availability of services may be based on areas

- Full list of venues that are "at risk" with details of the relevant time period (Hotspot QR Venues)

Analytical Data

Use of the app will start to populate the analytical data set. As noted above, most are summaries or counts of function use and do not list data items. The data is generated over the 6-hour analytical period and then prepared for submission.

All users will start to generate the following data items:

Core Details

- Start Date – when the period for the analytical data began
- End Date – when the period for the analytical data ended
- Postcode District – the current postcode district of the user
- Local Authority – selected by the app user based on their postcode district
- Device Model
- Operating System Version
- Latest Application Version

Data Usage of the app and data submitted to the app

- Cumulative Download Bytes (Data to App)
- Cumulative Upload Bytes (Data from App)
- Cumulative Cellular Download Bytes (Data to app by cellular)
- Cumulative Cellular Upload Bytes (Data from app by cellular)
- Cumulative Wifi Download Bytes (Data to app by wifi
- Cumulative Wifi Upload Bytes (Data from app by wifi)

Service and system checks

- total Background Tasks
- running Normally Background Tick
- completed Onboarding
- includes Multiple Application Versions

Function specific

The following data items are present for all users but vary by the functions used. Where not used the data, collected will only show a zero (or nil). So if you receive no test results all of the three test results fields will be zero.

Venue Check-In:

- Checked In (count of venue check ins)
- Cancelled Checkn (count of venue check ins cancelled - not check outs)

Test Results and reason (into the app):

- number of positive tests via Test Labs API
- number of positive test Token API
- number of negative tests Test Labs API
- number of negative test Token API
- number of void tests Test Labs API
- number of void test Token API

Pause functionality:

- Encounter Detection Paused Background Tick

Symptom Checker Use and Results:

- Completed Questionnaire And Started Isolation
- completed Questionnaire But Did Not Start Isolation

Isolation Trigger:

- Is Isolating Background Tick
- Has Had Risky Contact Background Tick

Isolation Analytical:

- Has Self Diagnosed Background Tick

- Has Tested Positive Background Tick
- Is Isolating For Self Diagnosed Background Tick
- Is Isolating For Tested Positive Background Tick
- Is Isolating For Had Risky Contact Background Tick

Exposure Window:

Exposure Windows are created to evaluate the risk of infection. In addition to being used within the GAEN, the data set is sent to the Product Environment and used in the Analysis of the app.

For each Exposure Window (see above for what triggers an Exposure Window) a 30-minute period of details are captured that contains:

- Exposure Windows: object
- Exposure Windows: date
- Exposure Windows: List of Scan Instances
- Exposure Windows: Risk score version
- Exposure Windows: Infectiousness of Index Case (i.e. the app user who shared their Diagnosis Key)
- Exposure Windows: Risk Score

Data Items to support analysis:

- Local Authority (Area)
- Postcode District (Area)
- Phone Model
- Operating System
- App Version
- Type of Event

Scan Instance (Exposure Window data sub-set)

Within the Exposure Window will be several scan instances that capture the distance and duration of the interactions in the following data items:

- Scan Instances: min Attenuation (an approximation of a minimum distance between app users)
- Scan Instances: Typical attenuation (an approximation of the typical distance between app users)
- Scan Instances: Time since last scan (a detail that allows the duration of a contact to be approximated)

Analytical Data upon arrival at the central system

No identifiers are provided to the data as it leaves the app, preventing a user from being identified across analytical data packets (subject to additional controls). On landing data will be placed into a row and time stamp of when the data arrived.

- Row Level
- Time Stamp

Processes used to prevent re-identification

The process of alerts for digital contact tracing prevents the app user being identifiable through data provided through the app's functionality. The matching of diagnosis keys with broadcast keys, that are derived from them, protects the identity and privacy of app users.

The following techniques are used to prevent re-identification of data received from the app (the analytical data set)

- Each data packet is sent each day without an identifier that would allow for the linking data of a user across multiple periods;
- Each device sends their data packets at a random time after the analytics window closes;
- Upon arrival information is removed from any data packet (such as the IP address), and processes are undertaken to protect the identity of users – such as small postcode district grouping and small number suppression;
- Further reviews and safeguards are in place for the performance view and data passed to the analytical environment.

Processes used to prevent re-identification (Exposure Windows)

In addition, the processes used above, the Exposure Windows are provided without any details of either app user such as the Diagnosis Key.

Scenario: App User has contact with Index Case

During a 14-day period, the app user has interacted with several other app users. The user's app collects the broadcast codes, which change every 15 minutes, of those other app users they have interacted with. This data is maintained with the GAEN provided by Apple and Google.

Alongside the broadcast code, data is captured about the Low Energy Bluetooth ("BLE") signal and its duration. This is used to approximate the distance and duration of the contact between the two app users.

Updated Diagnosis Keys

The app user receives the list of reference Diagnosis Keys. Other app user's who have tested positive for COVID-19, updated their status and chosen to share their Diagnosis Keys enable other app users to be appropriately alerted.

These Diagnosis Keys are added to the reference Diagnosis Key list provided to every app user. In order to help determine the infectious of a contact (the index case), this is accompanied by the onset of symptoms data from the app user sharing their Diagnosis Keys.

The app user receives the updated list, which is provided approximately every two hours, and their app checks whether any Broadcast Codes relate to any of these Diagnosis Keys. In this scenario, during the past 14 days an app user interacted with one of these index cases. The app finds a match, using the cryptography that preserves both user's identity, between a Diagnosis Key and Broadcast Codes.

Exposure Windows

The app uses the GAEN functionality and data to calculate the relevant risk score. This is done through the Exposure Window data set.

For each 30-minute window, whether partially or fully for 30-minutes, that the app user was in contact with the index case, an Exposure Window is generated and stored. This data set will include:

- The data of the Exposure Window;
- The risk score version used to calculate the risk score for the contact;

- The infectious of the Index Case (based on the onset of symptoms data provided alongside the Diagnosis Key);

- The risk score calculated for this Exposure Window;

- The list of scan instances within the Exposure Window.

The Exposure Window will cover at least one change in the Broadcast Codes (as they are changed every 15-minutes) but both will relate to the same Diagnosis Key.

Within the Exposure Window there will be Scan Instances for periods where the two app users were in contact. This is a summary of the BLE functionality that supports digital contact tracing.

These allow an approximation of the duration and distance of the contact and include the following data items:

- Scan Instances: min Attenuation (an approximation of a minimum distance between app users);

- Scan Instances: Typical attenuation (an approximation of the typical distance between app users);

- Scan Instances: Time since last scan (a detail that allows the duration of a contact to be approximated).

Analytical use of Exposure Windows

The Exposure Windows for the user are uploaded into the DHSC secure computing infrastructure and will be added to the app's dedicated analytical environment. The Exposure Windows are sent every 24 hours but are sent in a randomised schedule (so the first generated Exposure Window may not be sent via the Analytical API first) where applicable.

Once submitted, the Exposure Windows are prepared in the DHSC secure computing infrastructure and provided to the App Analytical Environment to enable analysis.

Analytical Data Set

The following examples, show what data is collected in two cases:

- Case 1 – The risk score from the contact is enough for the app to trigger an alert (recommending that the user self-isolates) it is above the risk threshold;

- Case 2 – The risk score from the contact is below the risk threshold and no alert is triggered.

Case 1 – Self-Isolation Recommended (Risky Contact)

In the case of a risky contact the app will alert the user. In addition to the data within the Exposure Window and Scan Instances data set, the analytical data set will include a summary and count of the interaction.

Isolation Trigger:

Is Isolating Background Tick – The Self-Isolation countdown will have been triggered by the Risky Contact, a count indicating that is the case for this day will be added (i.e. the value is returned as 1)

Has Had Risky Contact Background Tick – The app will capture the fact that you have had a contact which has reached (i.e. the risk score is greater than) the risk threshold set for a risky contact. The data set will indicate that this is the case for the day. (i.e. the value is returned as 1)

Isolation Analytical:

Is Isolating For Had Risky Contact Background Tick – The app will capture the fact that the app user is isolating for a risky contact (i.e. the value is returned as 1)

Case 2 – No recommendation (Non-Risky Contact)

In the case where the contact is not sufficient to trigger an alert, the app will capture the relevant Exposure Windows and Scan Instances providing them to the app's DHSC secure computing infrastructure. The analytical data set will include a summary and count of the interaction which differs from the case above in the following ways.

To show what data is captured, in comparison to the case above:

Isolation Trigger:

Is Isolating Background Tick – The Self-Isolation countdown is not triggered, a count indicating that is the case for this day will be added (i.e. the value is returned as 0)

Has Had Risky Contact Background Tick – The app will capture the fact that you have had a contact which has not reached (i.e. the risk score is greater than) the risk threshold set for a risky contact. The data set will indicate that this is the case for the day. (i.e. the value is returned as 0)

Isolation Analytical:

Is Isolating For Had Risky Contact Background Tick – The app will capture the fact that the app user is not isolating for a risky contact (i.e. the value is returned as 0)

Scenario: Venue Check-Ins

This example is a walkthrough of the use of the venue check-in function. This will help demonstrate what data is generated as a result.

Digital Contact Tracing

Venue check-in has no impact on the digital contact tracing function.

Data Held on the App

For each venue successfully checked into an entry is added to the app about each venue. It will include a time stamp of when the venue was booked into as well as an accessible description of the venue (i.e. its name and location). Deletion of these details is described above.

Analytical Data

Venue check-ins add a count of the venue check-ins during the 6-hour analytical period. Where the check-in fails or is abandoned this is counted as well. This data is used to ensure the QR venue check in is working as expected as well as give a sense of how app users are using the function and the potential impacts.

At the start of each day, both counts are reset to zero.

Venue Check-In:

- checked In (count of venue check ins);
- cancelled CheckIn (count of venue check ins cancelled - not check outs).

Processes used to prevent re-identification

Only those with access to the app will have details of the venues checked into. No details about which venues a user has checked into is included in the analytical data set or provided to the use.

Scenario: Contact Tracing Only (No Test Results sought, No Alerts Received)

You choose to just download the app and use it solely for contact tracing purposes. The app is only used for the baseline contact tracing.

The app is not used for any other purpose such as test results. They have not interacted with any other app user who tested positive for COVID-19, updated their app status and choose to share their diagnosis key alerting other app users (including you).

Outside of the app

If you test positive for COVID-19, the relevant Contact Tracing Team are likely to be in contact to establish who you have been in contact with and where you may have visited. This does not relate to your use of the app but is the normal manual contact tracing practice in public health emergencies.

In addition, if someone you know tests positive and they provide your details to the Contact Tracing team, this team will contact you. This will happen regardless of whether you have the app or not.

Digital Contact Tracing

In this scenario, the user is not generating any data from the use of the functions of the app.

Apple Google GAEN

As detailed for all app users. The app will hold the broadcast codes of other app users that the user has interacted with. As the users has received no alerts, none of the diagnosis keys within the reference set are relevant to the user. You would not receive an alert or a recommendation to self-isolate.

Data Held on the App

Your declared postcode district and selected local authority will be held on the app, along with all the reference material provided to every app user. There will be no venue or virology test results.

Analytical Data

The core details will be collected, in addition to the amount of data used and submitted by the app. The service and system checks data items will be present and populated, indicating that the app is working as expected.

Function specific

No function specific data will be generated for inclusion as the functions aren’t being used.

Risk of reidentification

By the data controller

The data collected from app users in this scenario and provided as part of the analytical data set include a minimal amount of data about the user and their use of the app.

The baseline risk of a reidentification (from small postcode district, rare phone make and model) is present but cannot be combined with other data associated with the app. No other data is held about the app user with a means of identifying them across systems. As

they have not sought a test via the app or returned results to the app, even the possibility of linkage to other data sets does not exist.

By other app users

As no alerts sent or received by the user, the app user will not be identifiable to other app users even outside of the app's functionality.

Scenario: Using all the app's functionality

You have downloaded the app and are using all of its functions. You use the app to routinely check symptoms, and where prompted will seek a test and add your test results to the app. When asked you choose to share details so that other app users can be alerted if appropriately. You use venue check-ins when prompted.

Outside the use of the app, the app user may be contacted separately to the use of the app. This will happen regardless of whether you have the app or not.

Digital Contact Tracing

The app user will provide their Diagnosis key when prompted to the central system. This will be provided to all other app users, so the risk the user is to other app users can be assessed and when needed alerts issued whilst maintaining everyone's privacy.

Apple Google GAEN

- Broadcast codes of other app users along with key details that allow the proximity and length of contact to be assessed. These are not accessible to you as an app user or us [Contacts Detected];

- List of Diagnosis Keys from the GAEN that were requested from user confirmed positive and shared with other users [Diagnosis Key Sets – reference material];

Data Held on the App

The app will hold details of all the venues checked into, unless deleted, test results and area of the user. The key differences with other app users will be the amount of venues listed and the current test result.

The same reference material is available to all app users.

Analytical Data

The set of analytical data will reflect the use of all the app functions. However, the data is a count or sum of data use. It will hold the: Core Details, Data Receipt and Transmission, as well as Service and system checks.

Function specific

All of the function specific data items will be collected. The combination may be particular to a user but (a) would, in part, reset every day and (b) be unable to be linked to the particular app user from the data retained.

For most data items, they are unlikely to be unique to any particular user. They cannot be linked to other data sets and would not identifiable in themselves.

Risk of reidentification

By the data controller

Despite the greater use of app functionality there is not a significantly greater risk of identification beyond the baseline. The data controller would need to know more details about the app user and their phone than is retained in the analytical data set.

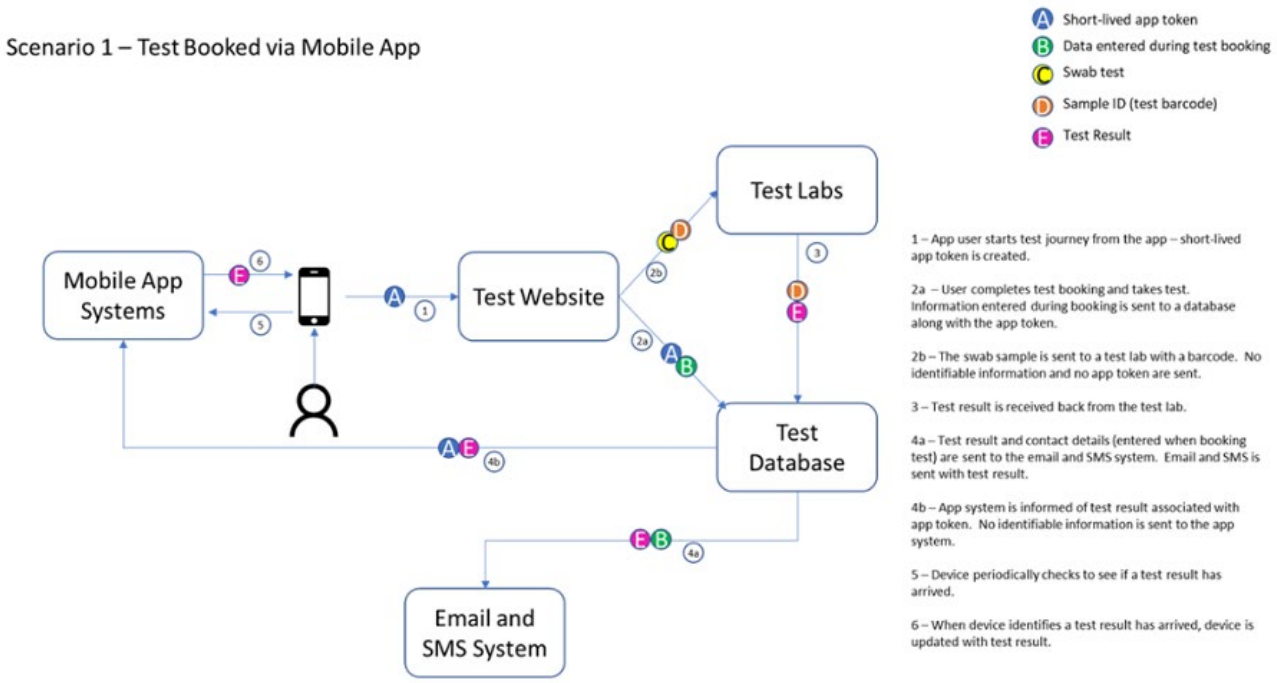
Protections in place to ensure that test results are appropriately returned are crucial for maintaining the privacy and identity of the user. This is supported by the prompt deletion of the test code once results are returned to the correct app user.

By other app users

Other app users would need additional information outside of the context of the app in order to identify another app user. The protections within the app ensure that the app ensures the privacy of all app users. In the “rural postman” scenario, an app user would have a limited number of contacts during the week and would be able to make an educated guess about which other app user had triggered an alert and has tested positive for COVID-19.

However, in such circumstances the individuals are likely to also be in contact with local Health Protection Teams (HPTs) and manual contact tracers. In such circumstances, which are routine for communicable diseases (as defined in law) and the COVID-19 public health emergency. The risk from users from the app is no greater and considerably less likely than the baseline risk of identification in public health situations which is necessary for the management of health risks to the public.

Scenario: Testing (via the App)



Scenario 1: Test Booked via Mobile App

You have used the symptom checker and have been recommended to take a test. The user generates a code through the app, which accesses the test code generating API. The test code is passed to the relevant testing website These websites are external to the app (and is treated as a separate “data ecosystem”) and data associated with testing is held separately to data about app users. The app token is short-lived and created specifically upon requested.

The swab sample taken from the user, whether at home or via on-site testing, is linked to a barcode no identifiable data accompanies the test and no app token is included (the app test code). The test results are returned to the person seeking the test via email and SMS (text message).

The app system is informed of the test result associated with the token (app test code). No identifiable data flows to the app from testing. The app periodically checks if a result is available, when it is the app is updated and the result deleted from the central systems once confirmed as sent to the correct app user.

The test result must be returned to the correct app user which is regardless of whether the result is positive, negative or void.

Returning the results and protecting the user's privacy

The technique used to provide app users with their correct result also ensure that the identity of the user is protected. When the app recommends a test for users it requests three separate tokens. These are generated by services outside of the app and are not recorded in the app. They are unique and anonymous and cannot be derived from each other or any other information. A secure database, used only for this purpose, associates these tokens and the three work together to maintain the privacy of users. Knowledge of just one token, particularly the CTA token, does not allow you to link results or trigger app functionality.

The three tokens are:

- The CTA Token which will go to the Virology website
- Test Polling Token is used by the app to check if a result is received
- Diagnosis Submission Token

Step 1. When the NPEx system returns a test result it includes the CTA Token. The app service looks up the Test Polling Token linked to the CTA Token and add the result to a database along with the Test Polling Token. The CTA Token is then deleted.

Step 2. When the app next checks to see if a result is available it submits the testing polling token, which can then be matched with the one held along with the result. Once the result is returned, the Test Polling Token is deleted.

Step 3. If you receive a post test result, you are asked to submit your diagnosis keys by the app. When you do the keys along with the Diagnosis Submission Token. This token is used to ensure that the keys are associated with a genuine result. Once you have submitted diagnosis keys the Diagnosis Submission Tokens is deleted.

All three tokens are retained in an App service secure database for only as long as needed. All three are sent to the app which stores the tokens in a Secure local store. The Test Polling Token, Diagnosis Submission Token and CTA Token are all created when the app asks for a CTA token when a user is recommended to take a test. All tokens are deleted once the test result has been delivered to the app.

Digital Contact Tracing

If you test positive for COVID-19 and receive or add your results to the app, you are prompted to share your diagnosis key with the app's central system. If you choose to do so, this key is added to the list of diagnosis keys provided to all app users.

Once received by other app users, the app's functionality (using the risk algorithm) combines with Apple Google's functionality to see if they need to be alerted.

This enables the app to check the broadcast codes it holds to determine if any are derived from any diagnosis keys in the reference pack. As broadcast codes change every 15 minutes, diagnosis keys are associated with the daily code and the checking mechanism is in the hands of Apple Google, the app user's privacy and identity is protected. The anonymity of the user is preserved from the DHSC (government) and other app users by the functionality of the app.

Apple Google GAEN

Data held will be in line with other app users.

Data Held on the App

In addition, to other data held on the app it will hold the app user's test result for the relevant isolation period plus 14 days. A positive test result will trigger the self-isolation timer to commence.

Analytical Data

For void or negative test results this will be added to the analytical data set. For positive test results this will also be included for a period of 14 days In addition, the self-isolation countdown will commence and relevant background checks will check in. These monitor the users compliance with isolation but are not used for enforcement and privacy safeguards prevent the app for being used for this purpose.

Relevant data items

Test Results (into the app):

- Received Void Test Result (test not conclusive)
- Received Positive Test Result
- Received Negative Test Result

Symptom Checker Use and Results:

- Completed Questionnaire And Started Isolation
- completed Questionnaire But Did Not Start Isolation

Isolation Trigger:

- Is Isolating Background Tick

- Has Had Risky Contact Background Tick
- has Self Diagnosed Positive Background Tick

Analytical Data upon arrival at the central system

No identifiers are provided to the data as it leaves the app, preventing a user from being identified across analytical data packets (subject to additional controls). On landing data will be placed into a row and time stamp of when the data arrived.

- Row Level

Processes used to prevent re-identification

Within the app and with contact tracing

The process of alerts for digital contact tracing prevents the app user being identifiable through data provided through the app's functionality. The matching of diagnosis keys with broadcast codes, that are derived from them, protects the identity and privacy of app users.

Within the analytical environment

No data specific to the test process, code or process (other than the result) is retained in the app analytical environment.

Within the testing system from website through to the return of the results

See above for how the use of tokens and testing system protects the identity of users.