Data Protection Impact Assessment
NHS COVID-19 App PILOT LIVE RELEASE Isle of Wight

Data Protection Impact Assessment ("DPIA") *COVID-19 App PILOT LIVE RELEASE Isle of Wight Version 1.0*	
Approved By	
Post	Data Protection Officer Department of Health an Social Care
Name	John Ryder
Signature	Email 06/05/2020 15:34
Date	06/05/2020

Version History			
Version	Description	Approved	Authors
V 1.0	Initial approved version	06/05/2020	Collaboration between NHSX App Cell; NHS England and NHS Improvement Corporate Information Governance; Government Legal Department.

INTRODUCTION

The COVID-19 App ("**App**") is a mobile phone application developed by NHSX that is designed to provide support for: COVID-19 self-diagnosis; alerting users who have come in contact with other users reporting symptoms; public health planning; and research, in the context of the COVID-19 public health emergency.

This DPIA applies to a live release of the App limited to the population of the Isle of Wight, prior to the planned national release.

The controller and partner organisations

For the purposes of this version of the App, the Department of Health and Social Care (for the Secretary of State) will act as controller for the processing of personal data that supports the functioning of the App. The legal entities that comprise NHS England and NHS Improvement will provide resources to support the processing. These are the NHS Commissioning Board (operating as NHS England), the Trust Development Authority and Monitor (together operating as NHS Improvement).

Rationale for this DPIA

The App is designed to preserve the anonymity of those who use it. It does **not** collect any directly identifiable information (for example, it does not collect name, telephone number, NHS number or GPS location data).

For the App to function a number of unique identifiers are necessary. These distinguish between individuals but do not reveal their identities. They are not connected to other identifiers outside of the App. They enable the components of the App – the App installed on the phone and a central database – to perform the their functions. These are: to recognise a device; record information about proximity encounters between devices; and to send and receive notifications.

The recording of information about a proximity encounter between two users of the App is enabled through Bluetooth technology. This does not record the user's location, but does enable instances of the App installed on peoples' phones to keep a log of proximity encounters with other users, albeit in a way that does not collect any information about a persons location. At no point is a user's identity capable of being captured or disclosed by the instance of the App installed on a phone, or the central database.

One function of the App is to issue a one-time use Reference Code which is used to facilitate the ordering of a diagnostic test by the user. The use of this code requires that is is associated with information that does reveal the subject's identity such as name and telephone number – but only outside the App. This is only done by organisations that manage and conduct the testing process. These organisations do not have access to the App or its data. In a future release, this code may be used to facilitate the reporting of test outcomes back to the App. This will not involve the disclosure of information that reveals users' identities back to the App, and this process will continue to preserve users' anonymity

Although the data that is processed by the App does not reveal the identities of the users, we consider that the set of unique identifiers that are necessary for its functioning relate to identifiable natural persons for whom there are direct and specific consequences arising from their use of the App. For this reason, we are treating the data as *pseudonymised* data – albeit it has never been capable of revealing an individual's identity. On this basis, although

3

an individual will not be identifiable from the data, the data will qualfy as personal data, and the GDPR applies.

Because the operation of the App involves the processing of personal data, as that term is defined by the GDPR, we have completed this DPIA. It describes the envisaged data processing operations; assesses whether those processing operations are necessary and proportionate in relation to the purposes for which the App is being deployed; and it identifies risks and appropriate mitigation of risks to users and other data subjects from those processing operations.

We recognise that public trust and confidence in the App is paramount to its success.   We also recognise that transparency around the functioning of the App and its privacy controls is key to engendering that trust and confidence.

Confidential patient information
We are working on the basis that information about health sympton that users report using the App may qualify as *confidential patient information*, in particular for the purposes of the Health Services (Control of Patient Information) Regulations 2002 (the COPI regs.). These regulations provide for the processing of confidential patient information in specified circumstances and establish that such processing is lawful despite any obligation of confidence owed – i.e. setting aside the common law duty of confidence. Regulation 3 provides for the processing of confidential patient information for purposes relating to communicable disease and other risks to public health.

We are doing so even though, as explained above, the data collected by the device will not inckude or be linked with information that reveals users' identities. Whilst the App involves the processing of health information (for example, where a user notifies the NHS, through the App, that they have symptoms of COVID-19 following completion of a self-diagnosis checklist), that health information cannot be associated with any existing patient data held by the NHS.

The processing of pseudonymised personal data in controlled environments by NHS organisations is not considered to breach confidentiality. However, it is recognised that the processing by the App involves:

- transmission of data in a distributed environment with direct involvement of the data subjects;
- communication between data subjects without their direct control (i.e. where unique identifiers, in encrypted form, are shared between two devices during a proximity encounter);
- submission of data to a central database again without the direct control of the subjects (proximity users); and
- consequent direct effect on users (i.e. notifications to users that they have been in proximity with infected users and may be at risk of infection).

We also recognise that the App must comply with human rights legislation in particular:

Article 8 - Right to respect for private and family life

4

1. *Everyone has the right to respect for his private and family life, his home and his correspondence.*
2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*

The Department of Health and Social Care, has determined that any interference with the private life of users caused by the operation of the App is (i) in accordance with the law (in that the public authority (DHSC) has a legal basis to carry out the relevant personal data processing, and has the vires necessary to operate a public health App); and (ii) is a necessary and proportionate measure in a democratic society, in pursuit of the legitimate aim of ensuring public safety. Our demonstrable compliance with data protection legislation and the common law duty of confidence underpin this.

Key Privacy by Design and Default Principles used by the App
The App was designed and will continue to evolve with the following principles embedded.

- It will collect the **minimal** amount of data necessary;
- Data does **not** leave the device without the permission of the user;
- All users' identities will be obscured to protect their identity;
- There will be no third-party trackers in the app;
- Proximity data is deleted from the App on users' phones when no longer required
- The user can delete the App and its data from their phone at any time. Although this will not result in the automatic deletion of data from other users' phones, such data will be deleted on the expiry of the local App retention period – currently 28 days.
- In accordance with the law, personal data will not be kept for longer than is necessary in the central database. The exact retention period for data that may be processed relating to COVID-19 for public health reasons has yet to be set (owing to the uncertain nature of COVID-19 and the impact that it may have on the public). In light of this, we will ensure that the necessity to retain the data will be routinely reviewed by an independent authority (at least every 6 months).
- Data in the central database (the Sonar Backend) will not be available to those developing in the App apart from in exceptional circumstances.
- Provision of any data from the central database will be subject to data protection impact assessment and establishment of legal basis for the disclosure.

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 also provide information, processed at an aggregated level, for the strategic management of the COVID response.

Beta Testing
BETA Testing is vital to ensuring the technical viability of possible solutions. For the App, a CLOSED BETA test took place on 08/04/2020 – 09/04/2020 and 16/04/2020 involving volunteers from RAF Leeming, following completion of a DPIA.

Purposes

| Fully describe what is the purpose of the project and how is the processing of information necessary to that work? | **Purposes**
The COVID-19 App is a mobile phone application developed by NHSX that is designed to provide support for: COVID-19 self-diagnosis; alerting users who have come in contact with other users reporting symptoms; public health planning; and research, in the context of the COVID-19 public health emergency.

The App is designed to preserve the anonymity of its users. It does this by using several codes that are unique to instances of the App installed on users' phones, but do not reveal a user's identity. These codes are essential to facilitate communication between devices, with the central database, and for messaging. They are not linked to any information that identifies the user, and **the user cannot access them**. These are:

• The Sonar ID: a code that is given by the central database when the user registers. This is used to uniquely reference the data on the user's phone, and the data submitted to the central database that provides the alerting service.
• The Transmitted ID: an encrypted version of the same code that is collected over Bluetooth by other App users' phones when they are close to a user's phone, and similarly collected by the user's phone as a log of your proximity with other App users
• The messaging ID: A messaging code used to alert you when you have been close to another App user that has reported having Covid symptoms to the App.

Installation of the App is voluntary.

The following purposes are supported by the App:

(i)   Logging of proximity encounters and alerting:
      a. recording proximity encounters between users of the App on their respective devices, using Bluetooth technology;
      b. user self diagnosis using a tool included in the App; |

c. submission by a user to a central database (the Sonar Backend) of the fact that they have symptoms, together with their proximity information – encounters with users in the last 28 days.

d. analysing that user's proximity encounters and matching their contacts with the unique identifiers of other users;

e. notifying those other users (where they have had a contact of sufficient proximity / duration) that they are at risk of having contracted COVID-19.

(ii) Data analysis for public health planning and pandemic response, such as resource planning and epidemiological modelling.

(iii) Using de-identified or anonymised data for scientific research and statistical analysis.

Why is the processing of personal data necessary?
The processing of data including identifiers that are unique to individuals (which therefore meets the definition of personal data) is necessary in order to uniquely recognise the instance of an App installed on a device. This is to enable communications between devices so that proximity encounters can be logged and so that the user can be notified when they have been in proximity with another user that has reported that they have COVID-19 symptoms.

How does the processing of personal data work in relation to the identified purpose?
In relation to the purposes identified above, the processing works in the following way:

Assignment of Sonar ID
Each instance of the App, and therefore user, is assigned a unique ID (the "**Sonar ID**"). A central database (the Sonar Backend) provides alerts to users when it receives information that a user who they have been in proximity with has or may have, contracted COVID-19.

Proximity encounters
The App uses Bluetooth technology to recognise and connect with other devices using the App. During a proximity encounter, the devices exchange their **Transmitted IDs** (i.e. the Sonar ID in encrypted form), together with a timestamp for the encounter, and radio signal information. The latter is used by the Sonar Backend when proximity information has been submitted, to derive the distance between the devices during the encounter.

Data about proximity encounters is stored locally on the user's device, for 28 days. User's cannot access this information. When a user self-diagnoses with, or reports the result of a positive test for COVID-19, or they have been alerted by the App that they have been in contact with someone with COVID-19, they are asked to upload their proximity encounter data for contact matching.

Contact matching
When a user submits the fact that they have COVID-19 symptoms with their proximity information, the following information is uploaded about each proximity encounter

- Transmitted ID – the encrypted Sonar ID of other App
- Timestamp for encounter
- Radio Signal Strength Indicator - the strength of the Bluetooth signal received by a device

Uploaded proximity encounter data is automatically analysed in the Sonar Backend. The make and model of the device (e.g. Apple iPhone 10) is used help interpret the data – as bluetooth signal strength varies between devices. The Transmitted IDs of the App instances of users that have been logged by the submitting user's device are decrypted, to reveal their Sonar ID.

Where an encounter is determined to be of sufficient risk on the basis of duration and relative proximity, the Messaging ID for the proximate user is obtained by matching to the unencrypted Sonar ID. Using this the messaging system notifies that user that they have been in proximity with someone who has reported that they have COVID-19 symptoms.

Self-diagnosis
The App includes a self-diagnosis tool which enables the user to assess whether they may have COVID-19 on the basis of their symptoms. If they do, they are asked to upload the symptom information from their device to the Sonar Backend, with the following commentary:

This information will be used anonymously to encourage anyone who has recently come into contact with you, and has this app installed on their phone, to self-isolate. Together we can help save lives, protect the NHS and stop the spread of coronavirus in the UK.

At this point their proximity encounter data will also be requested, and the contact matching process described above will be carried out.

The app includes status pages indicating:

- Amber – You have been near someone who has coronavirus symptoms (from alert)
- Red – Your symptoms indicate you may have coronavirus (self-diagnosis)

Users are given advice on what to do when these statuses arise.

As part of the self-diagnosis journey, the App includes a facility for a user to request a unique one-time use **Reference Number** from the Sonar Backend. When requested this is then presented to the user via the App. This is a unique identifier that can be used to request a test for COVID-19, as follows:

1. An app user self-diagnoses: they are provided with a phone number to call and a reference number.
2. The user calls the call centre, using an automated message they are asked to confirm they are residents of the Isle of Wight and that they will be asked for an IoW address
3. If the user passes through the automated system, they will be asked for personal details required for the testing and the app reference code. People calling from outside of the IoW won't be able to proceed (the call centre person on the phone will check this)

Stages 2 and 3 are outside the scope of this DPIA, as any data generated at these points will not be stored on the App or the App database. For the purposes of the Isle of Wight release, the reference number will not be used to link test results back to the App.

Research and public health management
Users are asked to provide their Postal Area – that is, the first portion (up to the space) of the users' home address postcode (e.g. SW1A) when they intially install the App. The App will not collect data about which postal district a user might be in from time to time as they move around.

The Postal Area data will be used for public health planning purposes, in conjunction with reported diagnoses and proximity information (for example, to help local NHS organisations to understand the spread of the disease in their area), and may also be used for research purposes

Performance data
During the limited release in the Isle of Wight, additional data will be collected about the App's performance and user interactions with the App. This data will be captured through the Microsoft AppCentre and will not include the SonarID or any other identifying information, and

	will not be linked with any identifying information. This data is collected to help us understand whether the App and the related infrastructure is functioning as intended. This is necessarily held on Microsoft servers away from our platform, as some of the metrics are for the inability to contact our service.

Nature of the data

Will the processing involve anonymised information[1]?	Data may be fully anonymised for public health planning, research or statistical purposes, if those purposes can be achieved without the use of personal data. Otherwise, data may be linked to Sonar ID with such additional protection that is required as an output of data protection impact assessment.
Will the processing involve pseudonymised personal data?	Yes. Through Sonar ID and other related identifiers, the data allows the individuation of users. However, it is processed in a form that in cannot be attributed to (i.e. reveal the identity of) a specific data subject without the use of additional information, so we are treating the data as pseudonymised.

The data with pseudonymous identifiers may be shared with NHS England and NHS Improvement who will process with powers under the notice issued by the Secretary of Stae under s. 3(4) of the Health Service (Control of Patient Information) Regulations 2002. |
| Will the processing involve fully identifiable personal data? | No. For the reasons given above, the data will not be processed in a way that will allow users to be directly identified. |

Assets

Does the proposal involve creating a new information asset?	Yes
The Sonar Backend supporting the App, which will be hosted on Amazon Web Servicee servers (with fall back from Microsoft Azure)
Does the proposal involve processing data held on an existing information asset or assets?	No
Is/are the asset owner(s) aware of the proposal	N/A

---

[1] anonymous information is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable

What is the timeframe for the project/programme/initiative?
(Please include commencement dates and any foreseen end dates)

The project that this DPIA covers is the live release of the App on the Isle of Wight commnecing 4th May 2020.

Controllers[2]

For the release in the Isle of Wight	NHS England	No – provides agency support
	TDA	No – provides agency support
	Monitor	No – provides agency support
	DHSC (for the Secretary of State)	Yes
Data Protection Officers and SIROs	**DHSC** DPO: John Ryder SIRO: David Williams	
Information Asset Owner	Matthew Gould, CEO, NHS X supported by Geraint Lewis, SRO	

Screening questions

Does the proposal involve any of the following – drop down list to include: ● National Commissioning Data Repository (NCDR) data ● Data pseudonymised by NHS Digital ● Aggregate data ● Anonymised data	● Aggregate data Where possible, data will be aggregated for public health planning purposes. ● Anonymised data The data collected by the App is pseudonymised – albeit having never been directly identifiable there is no lookup to users' identities. This data may be used for analytical purposes to support planning and research, with the results presented as aggregate numbers. Such processing will be subject to the safeguards applicable to research processing under (i) Article 89(1) GDPR; and (ii)

---

2 'controller' means an entity that, alone or jointly with others, determines the purposes and means of the processing of personal data

	section 19 of the Data Protection Act 2018.
Has processing of this nature already been captured and considered within a previous DPIA? If so, link to reference number	Yes – CLOSED BETA DPIA
Will the processing involve a large amount of personal data (including pseudonymised personal data) and affect a large number of data subjects?	Yes
Will the project involve the use of a new technology(ies) which might be perceived as being privacy intrusive? i.e. using biometrics, facial recognition, Artificial Intelligence or tracking (such as tracking an individual's geolocation or behaviour)?	Yes. 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 novel.
Will the processing introduce or make use of a new platform not currently in use?	Yes
In the absence of proper controls is there the risk that the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy (e.g. health records), unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage?	Yes. A security compromise could lead to a loss of confidentiality of health data, albeit health data that would only be attributable to Sonar IDs, and not to users' identities.
Does the proposal introduce difficulties in ensuring that individuals are informed or able to exercise their information rights?	No. The App will be accompanied by a privacy notice, and with a process enabling users to exercise data subject rights.
Is there the risk that data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data?	No
Will the processing of personal data occur without informing the individual of the processing?	No
Will there be processing of genetic data, data concerning health, sex life, racial or ethnic origin, biometric data, political opinions, religion or philosophical beliefs, or trade union membership?	Yes – health.
Will there be processing of data concerning criminal convictions and offences or related security measures?	No
Will the project involve the targeting of children or other vulnerable individuals	No

for marketing purposes, profiling or other automated decision making?	
Will personal aspects be evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles?	Yes – the App calculates a risk-score for an individual based on their recent contact with people who report that they have coronavirus symptoms.
Will the project include a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person (e.g. a recruitment aptitude test which uses pre-programmed algorithms and criteria)?	No
Will the processing result in you making decisions or taking actions against individuals in ways which can have a significant impact on them? e.g. decisions about an individual's access to a product, service, opportunity or benefit, or recruitment aptitude test based on automated decision making (including profiling)?	Yes – the App sends notification alerts to users as a consequence of the calculated risk-score based on their recent contact with people who report that they have coronavirus symptoms.
Will there be a systematic monitoring of a publicly accessible area on a large scale (e.g. CCTV)?	No
Will the processing include any data matching e.g. the combining, comparing or linking of personal data obtained from multiple sources?	Yes – linking of user's Sonar ID to "proximity data" submitted by other users by the central database (Sonar Backend)
Will the processing include any denial of service e.g. decisions about an individual's access to a product, service, opportunity or benefit which is based to any extent on automated decision-making (including profiling) or involves the processing of special category data?	No
Will personal data about individuals be shared with other organisations or people who have not previously had routine access to the data?	Yes – users may share the Reference code provided to them by the App for the ordering and processing of tests with NHS Business Services Authority (NHSBSA) and linked by them to a patient record, at the point at which a user telephones their call centre to request a test.

	None of that data will be shared back to the App. In a future release the outcome of the test (positive or negative) may be shared back to the App.
Will the project/proposal use personal data about individuals for a purpose it is not currently used for or in a new way?	No – this is a new initiative and does not use existing data
Will the project require you to contact individuals in ways which they may find intrusive? i.e. telephoning or emailing them without their prior consent.	No.
Are you using a Data Processor/third party supplier or is a service/processing activity being transferred to a new supplier/organisation (or re-contracted) at the end of an existing contract?	Yes. Amazon Web Services, Firebase, Microsoft (Azure) and Pivotal / VMware Tanzu. All are subject to appropriate data processing contracts which will restrict them to processing personal data solely on behalf of, and subject to the instructions of, NHS England and DHSC.

NB. If the answer to any of the above questions is Y, please complete the rest of the form. If all of the screening questions are answered N, the local IG team must still sign off the DPIA.

Personal data[3]

Why would it not be possible to do without personal data?	The functionality that the app facilitates requires that unique identifiers are used – principally the Sonar ID (AKA anonymous ID), Transmitted ID and Messaging ID (AKA Notification Token). Whilst these identifiers do not and cannot reveal the users' identities, they are essential to the provision of the service to the natural persons that they represent.
	The processing of App Users pseudonymous personal data is necessary to deliver information and alerts to potentially at-risk members of the public. It allows, when users choose, to provide information about their proximity to other users when they receive an "At Risk" alert or self-diagnose as having coronavirus.
	The App also includes the facility for users to request a one-time use code which they can use to order a diagnostic test. This code is given by the usrer with their personal details to for example a call center which will arrange for the test to be done. They may disclose this information to the test provider. The personal

3 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

	details that users provide are only used by organisations involved in providing the testing service and are not sent back to the App. These organisations do not have access to the App or its data. The summary process flow below presents the usage of the identifiers and associated attributes.

COVID Proximity App – operational stages and information flows

0. NHS COVID App and System Architectu...

5. WIP - Overview - External system linking

Stage	Information flow	Journey based questions
0.	No flow via app.	**When I download the app** ○ What is stored by the Apple App Store or Google Play? ■ The fact that you downloaded the app and which device you downloaded it to. ○ What is recorded in my browser history? ■ If you follow the link in the application to the explanation or advice pages on the NHS website, the address of the pages you visit will be recorded in the browser history on your phone.
1. Registration	1. Postal Area (first portion of postcode) entered on Local Application 2. Messaging ID requested by Local Application from the messaging provider 3. Messaging ID retrieved by the Local Application from the messaging provider 4. Sonar ID requested by Local Application from Sonar Backend 5. Sonar ID generated by Sonar Backend and sent to Local Application (Sonar ID used to	**When I register** ○ What is stored in the NHS database? ■ Your app user id ■ The make and model of your phone ■ A messaging service id for this app only, which the app will use to send you messages ■ Your home postal district - the part of your postcode before the space ○ What is stored on my phone by the app?

	generate Transmitted ID during periodic rotation) 6. Messaging ID, Postal Area and device Make and Model sent to Sonar Backend (make and Model is used to interpret signal strength data to classify encounters)	■ Your app user id ■ A messaging service id for this app only, which the app will use to send you messages

2. On-going use:
Proximity encounters and self-diagnosis
	1. For each encounter with Proximate Application the Local Application captures
	    • Transmitted ID (Proximate Application's encrypted Sonar ID)
	    • Timestamp for encounter
	    • Radio Signal Strength Indicator – the strength of the Bluetooth signal received by a device
	
	2. Proximity information deleted from phone after 28 days from encounter – rationale in attached:
	
	How long is data kept on phone diagra
	
	3. Symptoms entered on Local Application. If symptoms indicate COVID-19 diagnosis – stage 3
		When I have the app running
		○ What is visible to Bluetooth devices near me?
		■ Your temporary app user id for the day
		○ What is monitored by my phone?
		■ Power and data usage of the app will be monitored by your phone
		
		When I am close to someone else who has the app
		○ What is stored on my phone by the app?
		■ The other person's temporary app user for the day
		■ Information about how strong the Bluetooth connection was between the two phones
		
		○ What is stored on the other person's phone?
		■ Your temporary app user id for the day
		■ Information about how strong the Bluetooth connection was between the two phones

3. Submission of self-diagnosis and proximity information to Sonar Backend	1. COVID-19 Self-Diagnosis assessed and recorded on Local Application
	2. Symptoms and Onset of symptoms sent by Local Application to Sonar Backend
	3. Proximity information sent by Local Application to Sonar Backend – for each encounter with Proximity Application:
	    • Transmitted ID
	    • Timestamp for encounter
	    • Radio Signal Strength Indicator – the strength of
		When I update my symptoms?
		○ If I have no symptoms?
		■ Nothing
		○ If I have symptoms?
		■ What is stored in the NHS database?
		● The data stored in your phone about other phones you have been close to in the last 28 days.
		● The symptoms you have reported
		● The date your symptoms started

		the Bluetooth signal received by a device	
4.	**Alerts to proximity users from Sonar Backend**	1. Sonar Backend decrypts Transmitted IDs for each Proximity Application to obtain Sonar IDs 2. Sonar Backend links Sonar IDs to Messaging IDs and uses these to send alerts to Proximate Applications	When I get a notification that I have been in contact with someone who has symptoms? ○ What is recorded in my browser history? ■ If you follow the link in the application to the explanation or advice pages on the NHS website, the address of the pages you visit will be recorded in the browser history on your phone.
5.	**Deleting the app**		If I delete the app ○ What is still stored in the NHS database? ■ Your app user id ■ The make and model of your phone ■ A messaging service id for this app only, which the app will use to send you messages ■ Your home postal district - the part of your postcode before the space ○ What is stored on the phone by the app? ■ Your app user id ■ A messaging service id for this app only, which the app will use to send you messages
6.		Request for and issuing of Reference Token	

What are the required personal data? Please itemise them or supply a dummy sample, blank forms, screenshots from the prototype system etc.
The Data Dictionary is attached 📄 PDF 1. IMP - Reference - Data Dictionary (dowr

Extract below regarding Isle of Wight metrics

During the limited release in the Isle of Wight, additional data will be collected about the App's performance and user interactions with the App. This data will be captured through the Microsoft AppCentre and **will not include the SonarID or any other identifying information, and will not be linked with any identifying information.**
This data is collected to help us understand whether the App and the related infrastructure is functioning as intended. This is necessarily held on Microsoft servers away from our platform, as some of the metrics are for the inability to contact our service.

AppCentre Required Data
Minimum data required for Microsoft AppCentre to operate, as documented under the 'required' subheaders on https://docs.microsoft.com/en-us/appcenter/sdk/data-collected . For convenience these are
● Application secret (identifying the app to AppCentre)
● Installation ID (identifying the app instance to AppCentre)
● Application Properties - Version, Build
● SDK properties - Name, Version
● Operating System properties - Name, Version
● Device Configuration - Language and Country Code, Time Zone Offset
Capture

Completion of Postal District field
Whether the user entered their postal district data into the app
Completion of Permissions process at installation
Whether the user completed the process granting required permissions for the app.
Mobile Operating System
The operating system in use on the device
Failure to get Firebase Token
Whether the app successfully obtained a Messaging ID from Firebase
Failure of Device Registration
Whether the app successfully obtained a Sonar ID from the backend
Successful Device Validation
Whether the app received a validation message from the backend
Number of contact events transmitted
Per 24 hours. NOT linked to SonarID
Number of contact events received
Per 24 hours. NOT linked to SonarID

Please confirm that this is the minimum amount of personal data that is necessary.	The process has been reviewed to ensure that this is the minimum amount of personal data necessary.
Would it be possible for the controllers to use pseudonymised personal data for any element of the processing?	All of the data is meets the criteria for pseudonymisation in that it *cannot be attributed to a specific data subject without the use of additional information.* The controller does not hold any additional information that could be used to attribute (i.e. reveal the identity of) to a specific data subject.

If Y, please specify the element(s) and describe the pseudonymisation technique(s) that we are proposing to use.	The following pseudonymisation techniques are implemented: ▪ The App User has a Sonar ID that is not accessible to them ▪ The user's Transmitted ID (which, during a proximity encounter, is shared by the user's App with the other App in proximity) is an encrypted Sonar ID and changes periodically to further obscure its identity ▪ For each user, the Sonar Backend will only hold the Sonar ID, Messaging ID, Reference Code (if generated) symmetric key of the App user and (if uploaded because the user has been (self-)diagnosed with COVID-19 or has been in proximity with another (potentially) infected user) their proximity encounter data (i.e. Transmitted IDs of proximity users).

Scale and constituency(ies)

What is the scale of the processing (i.e. (approximately) how many people will be the subject of the processing?	c. 160,000
Please describe the constituency(ies).	The population of the Isle of Wight

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. The App will have its first live test prior to being released nationally.

Joint working controllership relationship and bases for lawful processing

Which controllership scenario(s) below apply(ies)?		Yes/ No
3. One Party is a Controller, supported by staff employed by any of the other Parties	One Party alone is responsible for determining the purpose and means of Processing to exercise its own functions and consequently it is the sole Controller. An employee of another of the Parties who assists with the Processing under the guidance, direction or supervision of the sole Controller is acting as an agent of the Party which has the function and which is the Controller.	**Yes**
DHSC (for the Secretary of State)	6(1)(e) exercise of official authority – common law powers[1], and underpinned by Health Service (Control of Patient Information) Regulations 2002 Reg. 3(1) and 3(3)(c)	**Controller**
NHS England / TDA / Monitor	Provide agency support for the DHSC – legal basis is that of the controller	**Agency**

Special categories of personal data

Will the processing involve personal data about: (Please tick all that apply.)	
● racial or ethnic origin	No
● political opinions	No
● religious or philosophical beliefs	No
● trade union membership	No
• genetic data[6]	No
• biometric data[7]	No

---

[1] R v Secretary of State for Health, ex parte C [2000] 1 FLR 627

[6] 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question

[7] 'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data

• data concerning health[8]	Yes
● data concerning the sex life or sexual orientation of the data subjects	No

If there are no special categories of data processed, please skip the following section and proceed to the 'Common law duty of confidentiality' section…

Conditions for processing special category personal data

Legal basis	Personal data to which this legal basis relates: All data processed by App.
● necessary for health or social care purposes	GDPR Article 9(2)(h)
Yes Underpinned by DPA 2018 – Schedule 1, Part 1, s. 2(2)(f) – Health or social care purposes	
necessary for public health (please specify below)	GDPR Article 9(2)(i)
Yes Underpinned by Regulation 3(1) and 3(3) of the Health Service (Control of Patient Information Regulations) 2002	

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.	The data collected by the App and uploaded to the Sonar Backend is being treated as if a common law of confidentiality is owed.	
Where it is planned to use or disclose such data, what are the grounds for doing so?	● consent ● safeguarding ● other overriding public interest - please specify	1. Consent – installation and use of the app is voluntary. Users understand that their proximity information will be captred by othe user's

---

[8] 'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status

	● legal duty or permissive power e.g. s251 support – please specify (e.g. court order)	phones and uploaded to the central database. 2. Regulation 3(1) and 3(3) of the Health Service (Control of Patient Information) Regulations 2002.
If the processing is of data concerning health or social care, is it for a purpose other than direct care[9]?	Public Health Management	

Consultation

Would it be appropriate to seek the views of data subjects or their representatives on the proposed processing?	Yes
If Y, how will this be done?	Consultation with an Ethics Advisory Board (chaired by Professor Sir Jonathan Montgomery from University College London who previously headed the Nuffield Council on Bioethics) and Focus Groups. User Accessibility Testing (via NHS X delivered by Pivotal / VMware Tanzu). See Terms of Reference for EAB and Focus Groups for further details.
If N, why is this the case?	
Would it be helpful to seek advice from independent experts (clinicians, security experts, ethicists etc.) where their specialist knowledge would be useful in understanding and managing privacy risks?	Yes. We have consulted with: • the National Data Guardian's Panel; • the Centre for Data Ethics and Innovation; and • representatives from Understanding Patient Data.
If Y, how will this be done?	As above
Will any other stakeholder(s) (whether internal or external) need to be consulted about the proposed processing (e.g. NHSE Central team, Public Health England, NHS Digital, the Office for National Statistics)?	ICO (to brief) National Data Guardian ("NDG") (part of the EAB, but also briefed separately)

---

[9] direct care: a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care.

What was/were the outcomes(s) of such consultation?	The consultation resulted in the creation of the independent ethics advisory board and in recommendations issued to the App Oversight Board. They were incorporated into the DPIA for CLOSED BETA and developed through subsequent iterations. Both CDEI and NDG offered thoughts and recommendations both of the functionality of the app (for example the use of self-diagnosis) but also the need for transparency and clarity on use of data. CDEI NHSx Board note 26-3-20.pdf

Datasets and access

Data within the Sonar Backend and flows into the Sonar Backend will be accessible and used by the COVID-19 Contact App team. Members of the team include:

- ▪ [via NHS X] Department of Health and Social Care, COVID-19 team;
- ▪ [via NHS X] NHS England staff working under the instructions of the Department of Health and Social Care, COVID-19 team;
- ▪ Staff working for Data Processors as outlined below.

Data processor[10]

Will the processing be wholly or partly performed on our behalf by a data processor(s)?	Yes
If Y please give details	Amazon Web Services ("**AWS**") Pivotal / VMware Tanzu – for support to COVID-19 team and exceptional access e.g. to fix problems Firebase – messaging provider Microsoft (Azure)
Where is the data to be processed by the data processor?	● In UK; or ● Outside UK but in EEA

---

[10] 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

If the processing is not completed by a data processor, please ignore the following questions and proceed to the 'Collection of personal data' section …

What assurance has been/will be sought about the/each processor's compliance with the GDPR?	Pivotal / VMware Tanzu need to complete the assurance checklist
Will the contract use NHS England's standard data processing agreement template?	No
Will the contract contain standard clauses to require compliance with the GDPR?	AWS - AWS GDPR DATA PROCESSING ADDENDUM Microsoft - Microsoft Online Services Data Protection Addendum January 2020 Firebase - verify Pivotal / VMware Tanzu - G-Cloud 11 contract
Will the contract contain clauses to address the secure transfer of the personal data to a successor data processor should this become necessary or upon the expiry of the term?	N/A

Collection of personal data

Will personal data be collected from the data subject?	Yes – 1. on registration (postcode area associated with Sonar ID) 2. proximity encounter data and symptom data will be collected directly from the data subject when submitted via the App. The Sonar ID will be generated centrally on the Sonar Backend.
Will personal data be obtained from sources other than the subject?	Yes – other app users. See below.
Will personal data be collected from a third party(ies)?	Yes – Proximity encounter data submitted by App users will contain the Transmitted ID of other App Users that meet the proximity criteria.
If Y, please identify the third party(ies)?	Other App users .
Is the provision of personal data obligatory or voluntary?	The provision of personal data (i.e. uploading of data to the Sonar Backend) is a voluntary action for App Users. The user has chosen to load the App onto their device and will choose to provide their proximity encounter data when requested to do so by an alert.
If obligatory, why/how is that the case?	The provision of personal data is never obligatory. However, if user A and user B have a proximity encounter,

	and user A chooses to upload data about their encounter, then the provision of that data was not speciically voluntary for user B.
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 proximity encounter data then opportunities may be missed to carry out proximity alerting for that user (and the other users with whom they had proximity encounters).

How will the personal data be collected in each case?			
Phase	Collector	Mode	Content
Contact App - registration (phone)	Sonar Backend	Communication from mobile phone to the sonar backend is via HTTPS RESTful micro services over TLSv1.2 with other security protections.	Registration details including Postal Area
Contact App (phone)	User's phone	Bluetooth	Transmitted IDs and timestamps obtained from proximity users
Contact App Alert	User's phone	Via Firebase messaging service Packet data is encrypted with the receiving user's security key so only they can decrypt it.	Alert of proximity of reported COVID diagnosis
Submit Symptoms and proximity information	Sonar Backend	Communication from mobile phone to the sonar backend is via HTTPS RESTful micro services over TLSv1.2 with other security protections.	Transmitted ID and timestamp of proximity users

Additional technical detail about the collection of data is included in Appendix 1.

Privacy information

How will the data subjects be informed of the processing of personal data about them?	App users will receive a privacy notice that explains what information will be collected, how it will be used, the rights available to them, and sources of further information.

Accuracy of personal data

How will we ensure the accuracy of the personal data (including their rectification or erasure where necessary)?	All identifiers are internally generated and their accuracy is therefore within our control. Make and model of device is collected in order to help accurately calibrate proximity information. We are reliant on the user's self-diagnosis, but symptom checker questions have been carefully designed with professional oversight. We are reliant on the user to submit their postal area, but can check that it is a valid postal area code.
How will we monitor the quality of the personal data?	See above.

Subject access and data subjects' rights

How will it be possible to provide a copy of the personal data processed about a particular individual to them (redacted as necessary) should they request access to this information? (If you are purchasing an information management system, you should consider including requirements in the specification about searching and subject access requests.)	This will require users to have access to their Sonar ID. With this they may be able to make a request which will be processed via the DHSC SRR process. The technical practicality of this needs to be assessed. If users do not have access to the Sonar ID, SRRs may be exempt under Article 11.
What processes will be put in place to ensure that other data subjects rights can be appropriately applied to the personal data if necessary?	As above. Users may uninstall the App from their phone at any time which will cause deletion of all the app data from the device. This will not cascade to the Sonar backend.

Data sharing

Will some or all of the personal data be shared with a third party.	The data may be shared with NHS England and NHS Improvement who will process with powers under the notice issued by the Secretary of Stae under s. 3(4) of the Health Service (Control of Patient Information) Regulations 2002.

If N, please skip outflows in the next section …

If Y, will the personal data be disclosed to a recipient(s) in a country outside the EEA or an international organisation?	No

Data flows - see Appendix 1

Risks

What are the identified risks of the processing?

20200505a DPIA Risk
Log Covid Proximity A

Please see risk register attached.

[Application security risk register redacted for publication]

Application security risk register – 29/04/2020

[Platform security risk register redacted for publication]

Platform security risk register – 29/04/2020

Incident reporting

What plans are in place in relation to the internal reporting of a personal data breach? (NB Unless the personal data breach is unlikely to result in a risk to the rights and freedoms of the individual(s), it will normally need to be reported to the ICO within 72 hours.)	DHSC's standard policies and procedures for personal data breaches will be followed.
What plans are in place in relation to the notification of data subjects should there be a personal data breach? (NB Where a personal data breach is likely to result in a high risk to the rights and freedoms of the individual(s), they should be notified as soon as reasonably feasible and provided with any recommendations to mitigate potential adverse effects.)	In the event of any breach, appropriate information will be sent to App Users though this functionality will not be available in Minimum Viable Product.

Business continuity planning

How will the personal data be restored in a timely manner in the event of a physical or technical incident?	For the Sonar Backend, appropriate back-up processes and procedures will be in place in line with standard G-Cloud contract requirements.

Retention of personal data

What is/are the retention period(s) for the personal data?	In accordance with the law, personal data will not be kept for longer than is necessary. The exact retention period for data that may be processed relating to COVID-19 for public health reasons has yet to be set (owing to the uncertain nature of COVID-19 and the impact that it may have on the public). In light of this, we will ensure that the necessity to retain the data will be routinely reviewed by an independent authority (at least every 6 months). There will be a research value for data selected by the NHS COVID-19 App, along with any other COVID-19 data set. Whilst the NHS COVID-19 App will ensure that information processed within the NHS COVID-19 App cannot be identified, there may be requests to process data from the app for research purposes, which may be linked with identifiable data. All such requests will be subject to further approvals and independent oversight.
What is the basis for this retention period? (Please indicate applicable guidance or rationale)	The retention period, including tha for individual data items will be reviewed on an ongoing basis.

Direct marketing[11]

Will any personal data be processed for direct marketing purposes?	No. Notifications sent to users do not constitute advertising or marketing material.

---

[11] direct marketing is "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals" - all promotional material falls within this definition, including material promoting the aims of not-for-profit organisations

If Y, please describe how the proposed direct marketing will take place:	

Data portability

Where the processing is based on consent or due to a contract, it is carried out by automated means and the data subject has provided the personal data to us, will it be possible to provide them or a different controller with the personal data in a structured, commonly used and machine-readable format? (NB This does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller – GDPR Article 6(1)(e)).	Not Applicable

Automated processing

Will the processing result in a decision being made about the data subject solely on the basis of automated processing[12] (including profiling[13])?	Yes
If Y, is the decision: ● necessary for entering into, or performance of, a contract between the data subject and a data controller ● authorised by law ● based on the data subject's explicit consent?	The processing is authorised by Regulation 3(1) and 3(3) of the Health Service (Control of Patient Information) Regulations 2002.
Please describe the logic involved in any automated decision-making.	See attached specification for the risk scroring algorithem 📄 PDF Risk-scoring Algorithm - For Public
Please outline the significance and the envisaged consequences of such processing for the data subject.	The NHS COVID-19 app uses Bluetooth to anonymously record the distance over time between people who have downloaded the App. If a person reports coronavirus symptoms,their recent history of interactions is uploaded to a central database and this algorithm is used to update the risk-score for

---

[12] examples include the automatic refusal of an online credit application and e-recruiting practices without any human intervention

[13] 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements

every app user they have come into contact with.

If the risk-score for an individual crosses a given threshold, they will receive additional guidance from PHE on how they can prevent the spread of the virus.

ICT

Will we, or the data processor(s), be using a new system to process the personal data?	Yes – developed by the Pivotal / VMware Tanzu

If Y to the above question around new systems, please ensure that a System Level Security Policy is completed and risk assessed by ICT before proceeding to the sign off stage below.

Appendix 1 – Data inflow and outflow tables

Inflows					
Sender	*Content*	*Pseudonymised?*	*Mode*	*Security*	*Recipient*
User	See Stage 1 Registration details	yes	Mobile phone app to Sonar Backend	Communication from mobile phone to the sonar backend is via HTTPS RESTful micro services over TLSv1.2 with other security protections.	Sonar Backend
Proximity User	See Stage 2 • Transmitted ID (Proximate Application's encrypted Sonar ID) • Timestamp for encounter • Radio Signal Strength Indicator – the strength of the Bluetooth signal received by a device	Yes	Bluetooth	Transmitted ID is encrypted with daily rotation	Local User

User	See Stage 3 for each encounter with Proximity App: • Transmitted ID • Timestamp for encounter • Radio Signal Strength Indicator – the strength of the Bluetooth signal received by a device	Yes	Mobile phone app to Sonar Backend	Communication from mobile phone to the sonar backend is via HTTPS RESTful micro services over TLSv1.2 with other security protections.	Sonar Backend

Outflows					
Sender	*Content*	*Pseudonymised*	*Mode*	*Security*	*Recipient*
Sonar Backend	Alert that the receiving user has been in contact with an infected individual	Yes	Via Firebase messaging service Packet data is encrypted with the reciving user's security key so only they can decrypt it.	Via Firebase messaging service Packet data is encrypted with the reciving user's security key so only they can decrypt it.	User