House of Commons
House of Lords

Joint Committee on Human Rights

Human Rights and the Government's Response to Covid-19: Digital Contact Tracing: Government Response to the Committee's Third Report of Session 2019–21

Ninth Special Report of Session 2021–22

Ordered by the House of Commons
to be printed 16 March 2022

HC 1198
Published on 18 March 2022
by authority of the House of Commons

Joint Committee on Human Rights

The Joint Committee on Human Rights is appointed by the House of Lords and the House of Commons to consider matters relating to human rights in the United Kingdom (but excluding consideration of individual cases); proposals for remedial orders, draft remedial orders and remedial orders.

The Joint Committee has a maximum of six Members appointed by each House, of whom the quorum for any formal proceedings is two from each House.

Current membership

House of Commons

Harriet Harman QC MP (*Labour, Camberwell and Peckham*) (Chair)

Joanna Cherry QC MP (*Scottish National Party, Edinburgh South West*)

Florence Eshalomi MP (*Labour, Vauxhall*)

Angela Richardson MP (*Conservative, Guildford*)

Dean Russell MP (*Conservative, Watford*)

David Simmonds MP (*Conservative, Ruislip, Northwood and Pinner*)

House of Lords

Lord Brabazon of Tara (*Conservative*)

Lord Dubs (*Labour*)

Lord Henley (*Conservative*)

Baroness Ludford (*Liberal Democrat*)

Baroness Massey of Darwen (*Labour*)

Lord Singh of Wimbledon (*Crossbench*)

Powers

The Committee has the power to require the submission of written evidence and documents, to examine witnesses, to meet at any time (except when Parliament is prorogued or dissolved), to adjourn from place to place, to appoint specialist advisers, and to make Reports to both Houses. The Lords Committee has power to agree with the Commons in the appointment of a Chairman.

Publication

Committee reports are published on the Committee's website by Order of the two Houses.

Committee staff

The current staff of the Committee are Andrea Dowsett (Lords Clerk), Busayo Esan (Inquiry Manager), Liam Evans (Committee Specialist), Thiago Froio Simoes (Committee Specialist), Alexander Gask (Deputy Counsel), Samantha Granger (Deputy Counsel), Eleanor Hourigan (Counsel), Natalia Janiec-Janicki (Committee Operations Manager), Lucinda Maer (Commons Clerk), George Perry (Media Officer), Nicholas Taylor (Second Commons Clerk) and Jackie Yu Hon Lam (Committee Operations Officer)

Contacts

All correspondence should be addressed to the Clerk of the Joint Committee on Human Rights, Committee Office, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 4710; the Committee's email address is jchr@parliament.uk.

You can follow the Committee on Twitter using @HumanRightsCtte

Ninth Special Report

The Joint Committee on Human Rights published its Third Report of Session 2019–21, Human Rights and the Government's Response to Covid-19: Digital Contact Tracing (HC 343 / HL Paper 59) on 7 May 2020. The Government response was received on 8 March 2022 and is appended below.

Appendix 1: Letter from the Secretary of State for Health and Social Care

Response to the Joint Committee on Human Rights report on Digital Contact Tracing

On 7 May 2020, you published a report on the Government's response to Coronavirus (COVID-19): Digital Contact Tracing, reviewing the plans to implement a contact tracing mobile phone app.

Thank you for undertaking the inquiry, and for raising your concerns and recommendations in the report. I must sincerely apologise for the length of time it has taken to provide a full response. The delay was due to an administrative error.

Please find attached our full response to your report.

The NHS COVID-19 app that was launched in September 2020 across England and Wales —and has remained in use since then—is a decentralised app, based on the Google/Apple API. It is significantly different to the centralised app that you considered in your report, and as such will have addressed some of your concerns.

The app has, from the start, been designed to the highest standards of data privacy and data security. It does not track individuals and the app does not hold personal information centrally.

We have worked closely with the Information Commissioner's Office and National Data Guardian at all stages of development, and continue to do so, to ensure the app meets their rigorous standards around user privacy and security.

Since the launch of the app, there have been over 30 million downloads across England and Wales, and over 11.6 million contact tracing alerts sent by the app in England, allowing citizens to act quickly to help protect those around them and limit the spread of the virus. More App statistics can be found here: https://stats.app.covid19.nhs.uk/ which may be of interest to you.

I hope you find this useful. If you have any further questions please do not hesitate to contact me.

Rt Hon Sajid Javid MP

Appendix 2: Government Response

Executive Summary

The Joint Committee on Human Rights carried out an inquiry into the government's response to coronavirus (COVID-19), with particular emphasis on government proposals for digital contact tracing, and the subsequent report was published on 7 May 2020.[1] In a letter to the Joint Committee of 20 July 2020, Lord Bethell, the then Parliamentary Under Secretary of State (Minister for Technology, Innovation and Life Sciences), welcomed the inquiry and undertook to provide a fuller response in due course. This is that response.

The Committee's report set out conclusions and recommendations across three areas: efficacy and proportionality; privacy and other human rights protections; and legislation. These related to the contact tracing app that was in development in spring 2020. On 18 June, however, the government announced the next phase of development of the app, which brought together the work done so far on the NHS COVID-19 app and the Google/Apple framework.

As a result of the change to a decentralised model, the NHS COVID-19 app that is now operating across England and Wales differs considerably from the model on which the Committee commented in May 2020. While the app has been designed from the start to protect the anonymity of users, the move to a decentralised model enabled even stronger safeguards to be incorporated in the design of the app. The NHS COVID-19 app has been designed using the Information Commissioner's Expectations for Contact Tracing Apps document,[2] puts privacy at its heart, retains minimal personal data only on the user's phone, and the use of the app is entirely voluntary. The user can also choose to delete the app at any time.

We believe that the NHS COVID-19 app has been developed in ways that accord well with the Committee's recommendations of 7 May 2020.

Introduction

Nearly every country in the world has been affected by, and experienced challenges in managing, coronavirus since it first emerged at the end of 2019.

The NHS Test and Trace service and NHS Wales Test, Trace, Protect aim to maximise how rapidly and accurately we can alert people who may have been exposed to the virus and give them appropriate public health advice, so as to limit COVID-19 transmission. The fundamental tracing component of the NHS Test and Trace service and NHS Wales Test, Trace, Protect is the dedicated contact tracing staff and public health experts, supported by online technology. These systems enable people who have tested positive for coronavirus to share information about their recent contacts, so that those individuals can be contacted and given appropriate public health advice to help limit the spread of the virus. The NHS COVID-19 app complements, and is part of, the NHS Test and Trace service and NHS Wales Test, Trace, Protect. It is designed to alert people who have had

[1] Human Rights and the Government's Response to Covid-19: Digital Contact Tracing, Joint Committee on Human Rights, Third Report of Session 2019–21, HC 343 / HL Paper 59

[2] ICO, COVID-19 contact tracing: data protection expectations on app development, 4 May 2020

close contact with someone who has subsequently tested positive but who it may not be possible to identify through standard contact tracing approaches, because the person who has tested positive does not know them or does not remember having contact with them.

The app team, as part of NHS Test and Trace, has worked constructively with Apple, Google, and many other organisations to develop and test the NHS COVID-19 app. The team has also worked with partners in countries including Ireland, Switzerland, New Zealand and Germany and is extremely grateful for their support and continues to learn from, and support, colleagues across the world.

On 18 June 2020, the Government announced that it was bringing together the work done up to that point to develop an app with the Google/Apple framework. The app that was developed and launched is based on a decentralised approach and uses the "Exposure Notification API (application programming interface)", a framework provided by Google/Apple. This app was piloted in August 2020 in the Isle of Wight, the London Borough of Newham and with NHS Volunteer Responders, and then rolled out nationally from 24 September 2020. As of 19 January 2022, over 30 million people have downloaded the app in England and Wales.[3]

Research during the pilot phase showed that privacy protection is very important to potential app users. Whilst the centralised app initially developed did provide such protection, we believe that moving to a decentralised model provided greater public assurance of this which is likely to have contributed to mass adoption. On national roll out of the app, potential app users were able to read blogs from the Information Commissioner and National Data Guardian setting out how they had been engaged by the app team during development.[4]

Overview of the NHS COVID-19 app's Digital Contact-Tracing

The NHS COVID-19 app is designed to make fast, accurate, digital contact tracing possible while protecting the user's privacy and identity. The app has been designed to use as little personal data and information as possible. All the data that could directly identify the user is held on their phone, is not stored centrally and is not shared anywhere else. Any data that is provided from the phone will always be anonymised or aggregated.

When someone downloads the app to their phone, the app generates a code that identifies the app's existence on that device. This code changes every day so that it cannot be associated with the user or their phone. From this code the app produces another randomly generated code every 15 minutes. This code is collected by the app installed on other users' phones when the user come into close contact with them and is held there for 14 days. There is no way for another user to tell that a code collected from a particular user's phone relates to them or their phone.

If an app user tests positive for coronavirus, they can choose to share their result anonymously. The NHS will then send alerts to other app users who have been in 'close contact', over the last few days. These alerts will never identify an individual. If the app user who tested positive booked their test through the app, the test result will come through to

[3] NHS COVID-19 app statistics

[4] Blog: Data protection considerations and the NHS COVID-19 app, 18 September 2020 ; National Data Guardian tweet, 24 September 2020

their app automatically. However, they still need to click 'share random IDs' before their close contacts can be notified. If the user agrees, their daily codes are uploaded to the central system. The central system then sends those codes to every app user's phone and each user's app will check for any matches. Where there are matches, the user gets an alert that they have been in contact with someone who tested positive and receive appropriate public health advice, for example to take daily lateral flow tests (fully vaccinated contacts) or self-isolate (unvaccinated contacts). The central system does not know who any user has been in contact with.

The NHS COVID-19 app is interoperable with similar apps in Gibraltar, Jersey, Northern Ireland, and Scotland (our "interoperability partners"). This means that all our digital contact tracing apps work across all interoperability partners and any app users across these partners get alerts, in their digital contact tracing app, when they are needed regardless of which partner app they are using.

Recommendations from the Committee and Responses

Efficacy and Proportionality

1. ***The amount of data the contact tracing app requires on the private and family lives of individuals is not justifiable if the app does not contribute meaningfully to the easing of lockdown restrictions and the combatting of Covid-19. Digital contact tracing will not be as effective if uptake is low. Uptake will be lower without user confidence in privacy protections - therefore robust privacy protections are themselves key to effectiveness of the app and the digital contact tracing system. Interoperability with other countries' systems will also be relevant to efficacy, not least to ensure that there is interoperability of systems in use on the island of Ireland. The Republic of Ireland has elected to use a decentralised app and if a centralised app is in use in Northern Ireland, there are risks that the two systems will not be interoperable which would be most unfortunate.***

Accepted

This recommendation related to an earlier app version that collected more data centrally than the current NHS COVID-19 app, which is built using a decentralised model where personal data remains on the app user's phone. England and Wales have a decentralised app, as do Scotland and NI, and these are interoperable with each other.

Privacy and Other Human Rights Protections

2. ***There needs to be established by law and with sufficient powers a Digital Contact Tracing Human Rights Commissioner who would not only exercise oversight with the appropriate powers but also be able to deal with any complaints from the public and report to Parliament.***

Rejected

Given the level of privacy protection inherent in the NHS COVID-19 app, the Government considers the existing legal framework and oversight by bodies, such as the Information Commissioner and the National Data Guardian, to offer robust protection to the public. The app does not collect personal data to be held by the Government, app users are not located more precisely than by their postcode district (which will contain around 8,000 households), and it is a fundamental principle of the app that it should be privacy protecting and voluntary for users.

3. ***The Government must not roll out the contact tracing app nationally unless the following protections are in place:***

a) ***Primary legislation: Government assurances about intended privacy protections for any data collected do not carry any weight unless the Government is prepared to enshrine these protections in legislation. A Bill would provide necessary legal clarity and certainty as to how data gathered could be used, stored and disposed of. It would also increase confidence in the app, increase uptake, and improve efficacy.***

b) ***Oversight: There should be an independent body, such as a Digital Contact Tracing Human Rights Commissioner, to oversee the use, effectiveness and privacy protections of the app and any data associated with digital contact tracing. The independent monitoring body should have, at a minimum, similar enforcement powers to the Information Commissioner, to oversee how data collected is being used and protected. To guard against mission creep it cannot be left to the Information Commissioner's Office to be the only body with powers of oversight or sanction; such an Office is not designed to monitor the significant rights-based implications that app based surveillance raises and, in addition, the Information Commissioner has been involved in the development of the app. Matthew Gould in his evidence to the Committee stated "However, we do not yet know exactly how it will work; we do not know all the consequences. There will be unintended consequences and there will certainly be some things that we have to evolve." In light of this, the speed of piloting and intended roll out, it is imperative that an independent oversight body be established immediately. It must also be able to receive individual complaints. The monitoring body must be given sufficient resources to carry out their functions.***

Rejected

As Lord Bethell, the then Parliamentary Under Secretary of State (Minister for Technology, Innovation and Life Sciences), set out in his letter of 20 July 2020, the Government does not consider that new legislation is necessary to govern contact tracing. We are confident that existing legislation and our commitment to transparency, security and privacy provide sufficient protection and clarity to the public.

Given the level of privacy protection inherent in the NHS COVID-19 app, the Government considers the existing legal framework and oversight by bodies, such as the Information Commissioner and the National Data Guardian, to offer robust protection to the public. The app does not collect personal data to be held by the Government, app users are not located more precisely than by their postcode district (which will contain around 8,000 households), and it is a fundamental principle of the app that it should be privacy protecting and voluntary for users.

c) ***Child Safeguarding: Particular safeguards should be applied to children under 18. Children's use must be monitored in relation to data collection and***

use of data. Misuse must be identified and rectified promptly. Interviews with children and parents (where appropriate) must take place in order to support children and act on any concerns.

Partially accepted

The app is available to children between the ages of 16 to 18. We refer to these as young app users. All app users are asked to confirm they are 16 or over during loading of the app. If the app user confirms they are under the appropriate age for the app they will receive an appropriate message and be unable to continue using the app. We do not collect any data on the age of our 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 Information Commissioner's Office 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 are supported by links from the app to details about other services in the NHS Test and Trace service, in England, and those determined by NHS Wales Informatics Service (NWIS), in Wales.

d) ***Efficacy review: The Health Secretary must undertake a review every 21 days on the digital contact tracing system. Such reviews must cover efficacy, as well as the safety of the data and how privacy is being protected in the use of any such data.***

The Health Secretary must report to Parliament every 21 days on the findings of such reviews.

Rejected

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 is done using data across the medical features of the app such as isolation status, swab test status and symptom questionnaire results.

If the app user receives a positive test result, contact codes stored on the phone are shared with other app users (via the Google/Apple Exposure Notification system) 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, it is necessary to have access to the user's relevant area (either postal district or local authority), exposure events and pause button usage. This data is used to validate that the level of alerts users receive are consistent with the wider risk environment and to calibrate the efficacy of the alert system. 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 which can only be used for approved public health purposes.

These methods of monitoring the working of the app mean that it is kept under continual monitoring as regards efficacy.

Security measures relating to data are tested throughout the delivery lifecycle for both the applications and backend services. Protective security monitoring and application behaviour monitoring are provided by Cyber Defence Operations Centre and a company acting under contract to the DHSC (Zuhlke Engineering). Whilst Zuhlke Engineering are not required to process any personal data and are not considered a data processor, they operate under strict contractual controls.

e) ***Transparency: The Government and health authorities must be transparent about how the app, and data collected through it, is being used. The Data Protection Impact Assessment must be made public and updated as digital contact tracing progresses.***

Accepted

The app's Privacy Notice and Data Protection Impact Assessment (DPIA) have been published and are regularly updated as the app develops. Additionally, we have published 'privacy information for young people' and 'privacy information easy read'[5]. All except the DPIA have been translated into Welsh. We have also published videos explaining the app's privacy protections.[6]

f) ***Time-limited: Any digital contact tracing (and data associated with it) must be permanently deleted when no longer required and in any event may not be kept beyond the duration of the public health emergency.***

Not applicable as no digital contact tracing data is held

Retention of data in the app varies according to where it is held and what kind of data it is. There are two places that data is held, the person's own phone and the DHSC secure computing infrastructure. The DHSC secure computing infrastructure only processes data that is confirmed as anonymised as it enters the infrastructure. The exception to this (if you start your test request journey in the app) is a test code and test results, which are held briefly - the test codes that link a test result to the app are only held in the DHSC secure computing infrastructure for long enough to send the app the test result. The test codes are deleted within 48 hours. Data relating to Covid-19 exposure is held for an amount of time related to the duration of a Covid infection. For example, diagnosis keys are retained on the user's phone for 14 days and are then deleted. Submitted diagnosis keys are retained on the DHSC secure computing infrastructure for 14 days and then deleted. This means that 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 and are automatically deleted after 21 days. This is to take into account the maximum typical incubation period of 14 days and the maximum typical infectious period of 7 days. These QR codes are only held on the user's phone and the user may choose to delete them at any time.

[5] UK Health Security Agency and Department of Health and Social Care, NHS COVID-19 App privacy information, 4 March 2022

[6] Department of Health and Social Care, NHS COVID-19 app protecting your privacy, 24 Sept 2020

The long-term retention of analytics data held in the secure computing infrastructure will follow the latest government advice and therefore may increase or decrease, but retention of records associated with the app are likely to fall into two categories:

- records used to hold organisations to account are held for 8 years
- records used to 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 Section 46 Code of Practice, Public Records Act and the statutory duties of the Department of Health and Social Care.

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. Data submitted by app users does not contain direct, indirect or consistent identifiers. However, limits for the retention of data sets and records need to be set even where it does not constitute personal data. This applies to the analytical data noted above.

Legislation

4. ***The current data protection framework is contained in a number of different documents and it is nearly impossible for the public to understand what it means for their data which may be collected by the digital contact tracing system. Government's assurances around data protection and privacy standards will not carry any weight unless the Government is prepared to enshrine these assurances in legislation. Such a Bill must include the following provisions and protections:***

a) ***Set out the clear and limited purposes of this app for data processing: Personal data may only be collected and processed for the purpose of preventing the spread of Covid-19. No personal data collected through the digital contact tracing app may be accessed for any other purpose. No personal data collected through the digital contact tracing app may be shared with third parties. There should be prohibition against data use for certain purposes such as legal proceedings, to support or deny benefits, data sharing with employers.***

Rejected

As noted above, given the level of privacy protection inherent in the NHS COVID-19 app, the Government considers the existing legal framework and oversight by bodies, such as the Information Commissioner and the National Data Guardian, to offer robust protection to the public.

The app has been designed to use minimal personal data. In all instances, the data required, used or stored is minimised to 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. Where postcode district and local authority combinations result in lower numbers of households, they are merged with adjacent postcode districts (in the same local authority) in our datasets.

No data is collected that personally identifies individual app users. The very small amount of personal data that is collected could not be used to demonstrate the user's identity. Consequently, it cannot be used in any form of legal proceedings as set out above. The use of the app is entirely voluntary, and the user can also choose to delete the app at any time.

b) ***Unless an individual has notified that they have Covid-19 (or have suspected Covid-19) and has chosen to upload their data, all personal data should only be held locally on the user's device and must be automatically deleted entirely from the app every 28 days.***

Accepted

As set out above, personal data is held locally on the user's device and is automatically deleted every 28 days (or 21 days in the case of QR check in data).

The NHS COVID-19 app collects analytical data to ensure the app is working properly, safely and helping manage the COVID-19 public health emergency. Fuller and more detailed information is available in the app's DPIA and Privacy Notice.[7]

c) ***Any personal data held centrally (e.g. following a diagnosis of Covid-19 or suspected Covid-19) must be subject to the highest security protections and standards. Human Rights and the Government's Response to Covid-19: Digital Contact Tracing 17***

Not applicable as no personal data is held

The app has been designed to be privacy-protecting and anonymous. It only collects the data necessary to enable the app to operate effectively and to support the pandemic response. No data that could identify users is held centrally. Fuller and more detailed information is available in the app's DPIA and Privacy Notice.[8]

d) ***Limit who has access to data and for what purpose: Data held centrally may not be accessed or processed without specific statutory authorisation, for the purpose of combatting Covid-19 and provided adequate security protections are in place for any systems on which this data may be processed.***

Accepted

The DHSC secure computing infrastructure database holds the anonymous analytics dataset specified in the Data Dictionary in the DPIA.

Analytics data 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.

[7] UK Health Security Agency and Department of Health and Social Care, NHS COVID-19 App privacy information, 4 March 2022

[8] UK Health Security Agency and Department of Health and Social Care, NHS COVID-19 App privacy information, 4 March 2022

The Department of Health and Social Care also collects data and publishes weekly statistics about the NHS COVID-19 app[9]. Due to the design of the app, all data collected is anonymous and reporting is aggregated.

e) ***Data held centrally may not be used for data reconstruction (i.e. where different pieces of anonymised personal data are combined to reconstruct information about an individual through piecing together multiple data sets).***

Accepted

The measures taken to assure anonymisation are set out in a separate published document, as well as the app DPIA.[10] Every effort has been made to ensure reidentification risk is minimised, so that app users cannot be identified by piecing together multiple data sets.

f) ***Data held centrally must be deleted where a user so requests and may not be held for longer than is required and in any event for no longer than 2 years. All data collected must be deleted once the public health emergency is over.***

Not applicable as no personal data is held

Users have a number of individual rights, such as the right to know what personal data is held about them. They can ask an organisation for copies of their personal information verbally or in writing. This is called the right of access and is commonly known as making a Subject Access Request. However, these rights are mostly only available when the data controller (in this case DHSC) holds information that can identify the user. As the app is designed to prevent DHSC being able to identify the user, DHSC will not be able to respond positively to any requests for access to personal data, or any other rights users may wish to make to us directly.

Users may, however, readily access personal data held on their phone, as there is a feature on the app that allows users to view the data held on the app. They can also exercise their right to object and be forgotten by removing the app, deleting the data held by the app, or deleting the list of individual venues they have visited within the app itself.

g) ***The Minister must undertake a review and report to Parliament on the efficacy and privacy protections relating to digital contact tracing every 21 days.***

h) ***Powers for a Digital Contact Tracing Human Rights Commissioner to ensure that authority has sufficient powers, staff and resources to oversee the roll-out of digital contact tracing, to look into individual complaints, to make binding recommendations on data protection, collection, storage, safety and use.***

Rejected

Given the level of privacy protection built into the app, and the avoidance of collecting personal data as a result of the decentralised model, this has not currently been deemed necessary.

Contact details of the DHSC Data Protection Officer are provided at the end of the app's DPIA should users wish to make a privacy- or data-related complaint.

[9] https://stats.app.covid19.nhs.uk/

[10] UK Health Security Agency and Department of Health and Social Care, NHS COVID-19 app: anonymisation, definitions and user data journeys, 4 March 2022

ANNEX B – Background on development of the NHS COVID-19 app

- In March 2020, NHSX began development of a contact tracing app, which then moved to NHS Test and Trace in May 2020 to support the wider Test and Trace strategy to help contain the spread of infection. The app that was initially developed primarily used a centralised approach whereby data is shared with a central server managed by the authority which carries out data processing and/or storage, allowing for greater data analysis. A pilot of V1 of the app was launched on the Isle of Wight on 5 May 2020. The centralised version of the app was designed from the start to preserve user anonymity and to have privacy and confidentiality at its core. It nonetheless gave rise to concerns about perceived risks to data privacy. Based on the V1 trial and the intention to roll out an app potentially based on that model in the following weeks, the JCHR published a report on 7 May on Human Rights and the Government's Response to Covid-19: Digital Contact Tracing raising concerns and recommendations over data and anonymity.

- On 10 April, Google and Apple announced they were developing an API to resolve technical issues around contact-tracing apps, which would require a move to a decentralised architecture, and without use of geolocation. Most data would be stored locally on an individual's phone and as little data as possible is shared with the NHS. On 6 May, development of a version of an app that met Google/Apple requirements commenced.

- Trials showed that V1 only picked up a small proportion of contact events on Apple phones. V1 was not detecting a high enough proportion of contact events to be defensible. Development of the centralised V1 App product stopped, and the Isle of Wight trial was wound up, pending the launch of a Google/Apple version of the app, V2.

- The app that was eventually launched is based on a decentralised approach and uses the "Exposure Notification API (application programming interface)" provided by Google/Apple that is now available on most smartphones. This app was piloted in August 2020 in the Isle of Wight and subsequently in the London Borough of Newham and with NHS Volunteer Responders. This was rolled out nationally from 24 September 2020.

- There is evidence to support the epidemiological impact of the NHS COVID-19 app, recognising that the app has contributed to preventing the spread of COVID-19 within the range of interventions deployed against the disease. A study on the epidemiological impact of the NHS COVID-19 app from its launch on 24 September 2020 to the end of December 2020 estimated it was used regularly by approximately 16.5 million users (28% of the total population), estimating that approximately 300,000-600,000 cases were averted by the app, noting that these findings supported the continued development and deployment of such apps in populations that are awaiting full protection from vaccines.[11]

[11] The epidemiological impact of the NHS COVID-19 app | Nature