👑 GOV.UK

1. Home (https://www.gov.uk/)
2. Coronavirus (COVID-19) (https://www.gov.uk/coronavirus-taxon)
3. Protecting yourself and others from coronavirus (https://www.gov.uk/coronavirus-taxon/protecting-yourselves-and-others)
4. NHS COVID-19 app: privacy information (https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information)

- Department of Health & Social Care (https://www.gov.uk/government/organisations/department-of-health-and-social-care)

Guidance

NHS COVID-19 app: privacy notice

Updated 24 September 2020

Contents

Alternative versions of this privacy notice
Introduction
How the app will help you
What data the app uses
What we ask of you
Our responsibilities
Further information

OGL

This document supports the national rollout of the NHS COVID-19 app and will be subject to ongoing review and improvement.

The NHS COVID-19 app supports the Test, Trace and Protect service in Wales and the Test and Trace service in England.

Alternative versions of this privacy notice

This is the privacy notice for the NHS COVID-19 app. We have also produced:

- a summary of the privacy notice for young app users (https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-privacy-notice-for-young-people)
- an easy read version of the privacy notice (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/920962/NHS_COVID-19_app_privacy_information__easy_read_.pdf), designed to be an accessible overview

You can read details of the NHS COVID-19 app in Wales (https://gov.wales/coronavirus) and the Test, Trace and Protect service it supports.

You can also read a data protection impact assessment and supporting documents (https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-data-protection-impact-assessment).

Introduction

This privacy notice relates to the national rollout of a mobile application (app) developed to contribute towards the response of the coronavirus outbreak. The app is part of NHS Test and Trace, overseen by the UK Department of Health and Social Care (DHSC).

The app helps people manage their risk of exposure to COVID-19 and identify and inform those who have been or may be at risk. This may be because of where they live, who they have been in close contact with or as a result of venues visited.

For more information on the definition of close contact see the description of the risk algorithm (https://covid19.nhs.uk/risk-scoring-algorithm.html).

App users will also be supporting the public health response to the pandemic by sharing information (on an anonymous basis) about whether the NHS Test and Trace Programme and app are working as expected. You will, for example, be helping us understand how many people are booking a test, or showing symptoms. By using the app and sharing this information, you will be making an important contribution to helping your community stay healthy and save lives.

The app tracks the spread of the virus, but does not track people. It provides important alert features that help manage risk and allow the user to take appropriate action, as well as helping us and local services better understand and manage response to the COVID-19 public health emergency.

You can learn more about what we mean by terms such as anonymous in this document (https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/anonymisation-definitions-and-user-data-journeys).

You can also see our privacy notice for young app users (from 16 to 18) (https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-privacy-notice-for-young-people) and our easy read privacy notice (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/920962/NHS_COVID-19_app_privacy_information__easy_read_.pdf).

How the app will help you

The app is designed to make fast, accurate, digital contact tracing possible while protecting your privacy and identity. It uses the minimum amount possible of your personal data.

Contact tracing depends on being able to determine who a person who has tested positive for COVID-19 could have infected. Manual contact tracing involves asking an infected person to remember who they have been in contact with; the person can only identify the people they know. The app supports contact tracing through your phone, without needing to know anyone's names or identities.

The app includes a notification feature which will alert you if you've been near another app user who tests positive for coronavirus, if your local area (postcode district) has a changed risk status, or if you have visited a venue, which later reports an outbreak whilst you were there. If you test positive, the app will ask you to allow those you've been in contact with to be alerted. It uses technology developed by Apple and Google called 'exposure notification' and 'exposure logging' to do this. The people notified will not know who you are.

The app also allows you to:

- view current risk in your local area
- keep a personal record of venues visited where you 'check-in' using the official NHS QR code poster
- check whether any symptoms you have could be COVID-19
- order a test, via a link to the NHS Test and Trace website
- count down how many days you have left if you need to self-isolate

Future versions of the app may include additional features to help you to keep track of risk you personally are encountering, day-to-day.

What data the app uses

The app has been designed to use as little personal data and information as possible. All the data that could directly identify you is held on your 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, to prevent us and anyone else from identifying you or others.

You can read more about how we protect data through anonymisation (https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/anonymisation-definitions-and-user-data-journeys).

When you first install the app from your app store there will be instructions for you about how to allow the app to function. This includes turning on your Bluetooth settings (if not already on), entering the first part of your postcode (up to the space), which is also called the 'postcode district', and allowing notifications:

- Bluetooth is needed because the app uses the strength of the Bluetooth signal, the Low Energy Bluetooth function, to work out how near app users are to each other
- your postcode district, this is the first part of your postcode before the space, is needed so that the app tell you about the current risk level in your local area
- notifications are needed so you can receive alerts if the app identifies that you may have been in contact with someone who tested positive, or if there is a change to the public health risk level in your local area (postcode district), or a venue where you checked-in has had an outbreak when you were there. You can turn off notifications at any time in your settings.

Digital contact tracing

When you download the app to your phone, the app will generate a code that identifies the app's existence on your device. This code changes every day so that it cannot be associated with you or your 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 you 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 your phone relates to you or your phone.

If you receive a positive test result for coronavirus, the app will ask for your permission to share your daily codes with other app users. If you agree, your daily codes will be uploaded to the central system (the DHSC secure computing infrastructure, hosted on Amazon Web Services (AWS) UK and Microsoft Azure Cloud Services (UK)). The central system will then send your codes to every app user's phone and each user's app will check for any matches. Where there are matches, the user will get an alert that they have been in contact with someone who tested positive. The central system does not know who you have been in contact with and it doesn't record any matches.

While it is unlikely ever to happen, you should be aware that there are some unlikely circumstances in which another person might be able to identify that you were the person, who had tested positive when they receive an alert. If an app user had only been in contact with you and no one else, they would be able to infer who the infected person was when they received an alert. This could also happen with manual contact tracing.

The app uses automated processing to advise users, who have been in close proximity to those who tested positive, to self-isolate. The app will do this based on the risk of encounters you have had with other users who have tested positive. This will take account of factors such as the duration of time you spent with those other users and how close you were to them. You can read more about how this works (https://covid19.nhs.uk/risk-scoring-algorithm.html).

In appropriate cases the app will automatically send a notification recommending self-isolation. These notifications are private to the app user, so no one else will know that you have been advised to self-isolate, unless you choose to tell them.

The app reminds users that they can phone NHS 111 if they would like to discuss the advice to self-isolate. It is appropriate to call NHS 111 if you have any questions or concerns about your circumstances, what the alert means for you or what you need to do next (including whether it is appropriate to obtain a test).

This section of the app also includes a count down, so you can see how long you need to self-isolate, and further information and support to help you when self-isolating.

Your symptoms and ordering a test

If you choose to check your symptoms using the app, the symptom information that you enter will be processed by the app, but the app will not tell anyone else your symptoms.

If the app advises you to take a COVID-19 test, you will be directed to the NHS Test and Trace website to book a test. The NHS Test and Trace website will open in a new window. This website will collect your contact details (in order to be able to provide the test) but this information will not be shared with the app.

Booking a test via the app will generate a test code that will allow you to link your test result to the app automatically. If you test positive the app will ask you to share your anonymous contact tracing codes with other app users. The test codes that link your test result to your app are only held in the DHSC secure computing infrastructure for long enough to send your app your test result. The test codes are deleted within 24 to 48 hours.

Venue check-in

When you use venue check-in for the first time, it will ask you for permission to use the camera on your device in order to 'check in' to venues, which display the official NHS QR codes. If you check into a venue, information about the venue you've been to will be stored on your phone as a record, which you can review at any time over a rolling 21-day period.

This will include details of the venue and the time of your visit. However, these details are only stored on your phone.

If a venue you check into is subsequently identified as high risk, your app will alert you. You will also be able to use your venue check-in to remind you where you have been, if you are talking to a contact tracer after testing positive.

Unless you choose to disclose this information to a contact tracer, this information is private to you and will not be shared with anyone else. You have the option to delete this information at any time by removing either the whole record, or record of individual venues from the list held on your phone.

Helping the public health response

When you use the app you will be helping your community stay healthy and save lives by sharing important information about coronavirus in your region and how well the NHS Test and Trace Programme and the app are working. The app supports this in the background by sending anonymous information about activity to us. Sharing this information is an essential part of the contribution you make to the public health response when you download and use the app, as it helps us actively research, manage, plan and respond to the COVID-19 Public Health Emergency across the country and in your local area.

This information is also important to ensure the app is safe to use - providing accurate and effective public health related advice, information and support to app users.

You can read more about what information is accessed from your phone and how it is used for these purposes in the section 'Compliance with the Privacy and Electronic Communication Regulations'.

Your personal data

'Personal Data' is a term defined in law.

The following types of data are considered 'personal data' when they are on your phone, because they are being stored on a phone that is registered to you personally:

- the postcode district you provide when you install the app
- the symptom information you enter onto the app
- the QR codes of the venues that you scan into the app

- the 2 types of codes described above, which are generated every day and every 15 minutes respectively for contact tracing purposes

The app has been designed to ensure that before any of this data moves out of your phone, for example into the DHSC secure computing infrastructure (see below), there is no way of telling that it came from your phone or that it relates to you.

If you request a test code and obtain a test result, this information will be personal data both when it is on your phone and when held within the central DHSC systems. DHSC has established strict controls of security, access and systems to monitor and restrict who can have access to this information and prevent anyone from being able to identify you.

The status of your data

The data held on your app is considered personal data but is only accessible to you.

Data within the app's analytical data set has all direct identifiers removed and we aim to make your use of the app anonymous. As noted above, the IP address is removed and is not retained. The data items within the data set are a summary or count apart from Postcode District, Test results and the technical details.

The analytical data set supports all of the purposes outlined within this privacy notice with some data items supporting technical evaluation, others public health and many both.

See our user data journeys (https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/anonymisation-definitions-and-user-data-journeys) for more detail.

What we ask of you

As a user of the app we ask you to:

- download the app and use it daily
- keep the app 'on' and carry your phone at all times when you are able to
- follow instructions issued by the app
- 'pause' contact tracing by the app when appropriate
- enter symptoms and take a test quickly when advised to
- self-isolate (as we expect of everyone) if you test positive for COVID-19

The app will ask you to do these things, but it will not compel you in any way and no one will know anything about your personal use of the app. It does not record or track where you or other app users are (for example, at home or in a public space). The app does not identify you or your location to other app users. You can delete the app at any time, you can also choose to delete the data held on the app or just individual venues you checked into. If you delete venue details you will not receive relevant alerts about that venue.

Our responsibilities

We will adhere to our legal responsibilities. The legal basis for processing your personal data under the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018 law is:

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

- GDPR Article 9(2)(g) – the processing is necessary for reasons of substantial public interest in the basis set out in Part 2 of Schedule 1 of the Data Protection Act 2018 (para 6 (*Statutory and government purposes*))
- GDPR Article 9(2)(h) – the processing is necessary for medical diagnosis, the provision of health treatment and management of a health and social care system
- GDPR Article 9(2)(i) – the processing is necessary for reasons of public interest in the area of public health
- DPA 2018 – Schedule 1, Part 1, Section 2(2)(f) – the management of health care systems or services
- DPA 2018 – Schedule 1, Part 1, Section 3 – public health purposes

We will continue to develop the App following the Information Commissioner's (ICO) Contact Tracing Principles.

You can delete the app at any time and/or turn off notifications. If you choose to delete the app, you will not receive any notifications (alerts) from the app about coronavirus (COVID-19) and the data stored by the app on your phone will be deleted. If you decide to install the app again, you will need to provide the requested information again.

We will never share your personal data without your permission, and we will only process it as described in this privacy notice.

Under Article 22 of GDPR, we considered whether the app uses Automated Decision Making (ADM) as part of its processing of data. We consider that it does not but have complied with the legal and policy framework around Automated Decision Making and will continue to do so. We are taking all steps required to comply with these requirements.

There is more information in the Data Protection Impact Assessment (DPIA) (https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-data-protection-impact-assessment) prepared for the app by DHSC.

You can find our Appropriate Policy Documentation (APD) (https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-our-processing-of-special-categories-of-personal-data) setting out what special categories of personal data we process and why. We explain why we process this data whilst protecting your privacy. More detail can be found in our DPIA (https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-data-protection-impact-assessment).

Compliance with the Privacy and Electronic Communication Regulations (PECR)

The app requires access to data stored on your phone and stores data on your phone. Regulation 6 of PECR governs how we access this data which is only shared accessed strictly necessary to provide those services delivered by the app and set out in this privacy notice as further explained below.

Function: all features

In order for the app features set out in the rest of the table to function safely, we need to collect the following information from your phone:

- phone model
- operating system version

- app version number
- completion of onboarding
- storage usage
- data download usage
- usage status

We need to know this information in case any features of the app do not function correctly on specific phone models or operating systems, so we can quickly remedy the issue and/or alert relevant users. This is necessary to ensure the app provides the working functionality you need to stay safe.

We also need to validate that you are using an up to date version of the app and have completed the onboarding process. This is necessary to ensure you are using the app safely and have the benefit of the latest guidance and support the app offers.

We need to know the storage and data download usage that the app is using. This is necessary to ensure the app is able to function and not using disproportionate amounts of storage or data.

We also need to validate that the app is properly receiving updates from our systems. We do this every 2 hours to ensure you have access to real time risk information. This is necessary to ensure you have access the latest safety information.

Function: medical device efficacy and safety requirements

The app constitutes a medical device. To support accreditation as a medical device we are required to collect analytical data relating to:

- symptom questionnaire results
- isolation status
- swab test status

This information is necessary to ensure that the medical features of the app are working properly – for example we routinely cross check swab test result levels with our isolation advice to ensure the app's isolation advice is functioning correctly.

Function: check in to a venue

This function does not require any data to be collected in addition to that listed already.

Function: symptom checker

This function does not require any data to be collected in addition to that listed already.

Function: isolation countdown

This function does not require any data to be collected in addition to that listed already.

Function: digital contact tracing

For the contact tracing functions within the app to operate effectively we need to validate that the level of alerts users receive are consistent with the wider risk environment. To calibrate the alert system in this way, it is necessary to have access to the following information:

- postal district
- exposure events
- pause button usage

Function: public health response

The following information allows us and public health authorities to learn more about the virus and its transmission and take effective measures to manage the response to the COVID-19 public health emergency:

- postal district
- exposure events
- QR check in count
- symptom questionnaire results
- isolation status
- swab test status
- pause button usage

By way of example, having information about exposure events within postal districts will help identify us identify and manage areas of increasing risk around the country and to see if exposure events are happening at the expected levels, whilst information about the pause button is being used, gives our understanding of how many exposure events are taking place in context.

The provision of this information constitutes the valued contribution you will be making to the COVID-19 public health emergency response when you choose to download and use the app.

Data collected by DHSC to support these functions will be uploaded regularly from the app to a dedicated analytical area as explained in the following section. All data in the analytical area will be held in a format that does not identify an individual app user.

The DHSC secure computing infrastructure

The app is supported by a central DHSC secure computing infrastructure. Data in this DHSC secure computing infrastructure will be made available only to individuals that have been formally authorised to access it. Information will only be able to be transferred from this DHSC secure computing infrastructure to another system if appropriate, and after an updated Data Protection Impact Assessment has been carried out.

The DHSC secure computing infrastructure only processes data that has been anonymised once it enters the infrastructure, with the exception of a test code and test results which are held briefly. The test codes that link your test result to your app are only held in the DHSC secure computing infrastructure for long enough to send your app your test result. The test codes are deleted within 24 to 48 hours.

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. With these controls, monitoring and safeguards in place we conclude that the risk to data privacy of an app user being identified by a combination of factors (e.g. phone model and operating system, plus postcode district), would be negligible to non-existent.

Any use of data and information generated or collected by the app will comply with Data Protection law and the Common Law Duty of Confidentiality (where applicable).

Retention of data

Data held in the DHSC secure computing infrastructure will not contain direct, indirect or consistent identifiers. This means that the retention of this data should not be considered within the legal context of GDPR/data protection. However, limits for the retention of data sets and records need to be set even where the data does not constituent personal data. This applies to the analytical data explained above.

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

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

Retention of these records is governed by the relevant Section 46 Code of Practice, Public Records Act and statutory duties of the organisation accountable (DHSC).

Most data is retained only on the user's phone. Daily codes (the ones used for contact tracing) are retained on the user's phone for 14 days and are then deleted (14 days is the incubation period for the virus). Submitted daily codes are retained on the DHSC secure computing infrastructure for 14 days and then deleted. So, the maximum age of a daily code that has been distributed to the DHSC secure computing infrastructure is 28 days.

The test codes that link your test result to your app are deleted within 24 to 48 hours.

QR codes that are scanned by the user when visiting venues are automatically deleted after 21 days. The choice of 21 days takes into account the 14-day incubation period, and the infectious period of the virus.

The retention settings will follow the latest government advice and therefore may increase or decrease. For example, the self-isolation period recently increased from 7 to 10 days.

Your rights under the Data Protection Act 2018 and GDPR

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

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

As the app user is not identifiable within the DHSC secure computing infrastructure, we have aimed to provide you with functionality within the app where-ever possible. Once data is received by app's DHSC infrastructure we ensure that app users cannot be identified.

Right of access and requests for information

You can access key information through the app. Access the 'About this app' screen, then from the 'Your data' section click the link 'Manage data'.

Right to be forgotten

You can choose to delete the app and the data it contains.

Right to object

You can choose to delete the app, the data it contains or specific venues.

Automated individual decision-making including profiling

If you have concerns about the app's recommendations to self-isolate or seek a test, you are advised to contact NHS 111 (or the equivalent in Wales) or appropriate health care professional.

The right to data portability does not apply as the lawful basis is not consent or a contract. See the DPIA for more detail. The right to rectification and restriction of processing is not available due as we cannot identify app user's data within the DHSC infrastructure.

Information about your rights and how to use them is available from the Information Commissioner's Office.

Please note that the DHSC secure computing infrastructure does not hold any personal data about app users, except for any test codes and test results. It will not be possible to inform app users about their test code and result because it would require DHSC to collect further information and personal data just in order to satisfy this right. It would also undermine the privacy protection afforded to this data for the limited time that it is stored in the cloud.

If you are unhappy or wish to complain about how your information is used as part of this app, you should first contact the DHSC Data Protection Officer (DPO) to resolve your issue (see DPO section). If you remain unhappy, you can complain to the ICO.

Further information

If you would like more detailed information about the app, you can find this in the Data Protection Impact Assessment (https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-data-protection-impact-assessment) created for the app.

For more general information about coronavirus, please go to GOV.UK/coronavirus (https://www.gov.uk/coronavirus).

Data Controller

A 'Data Controller' is the organisation that is legally responsible for deciding how and for what reason a user's personal data is processed. For the NHS COVID-19 app, the Data Controller is the government Department for Health and Social Care (DHSC). Data Controllers have a 'Data Protection Officer' who acts as a contact point for questions about your data. Details of DHSC's Data Protection Officer can be found at the end of this information.

The app is being overseen by NHS Test and Trace, which is part of DHSC. DHSC has contracts or agreements with some other organisations that provide services in developing or supporting the app. The ones that will be processing personal data are:

- Amazon Web Services (AWS) which hosts the central system (cloud server) that supports the app
- The Health Informatics Service (THIS), which is hosted by the Calderdale and Huddersfield NHS Foundation Trust. THIS provides the 'NPEx' system which provides test results to the app (using the test code unique to the app)

These organisations can only work under instruction from DHSC and cannot use information they process for any other purposes.

These organisations' details can be found in the DPIA (https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-covid-19-app-data-protection-impact-assessment).

Data Protection Officer (DPO)

The DHSC Data Protection Officer for DHSC is Lee Cramp, who can be contacted by sending an email to data_protection@dhsc.gov.uk.

Security of your information

The system gives a high level of privacy protection, as the app does not collect or transfer any information that tells us who or where you are. This also means it cannot tell the NHS, people and organisations who have contributed to the development of the app, or any other app user, who or where you are.

In addition to the protections already explained above, we have implemented and maintain the necessary technical and organisational security measures; and Policies and Procedures.

These are designed to reduce the risk of:

- the deliberate or accidental destruction of data
- the loss of data
- unauthorised access to or disclosure of the information collected by the app

This includes:

- limiting access to those who can support the management of the app
- using secure, privacy preserving methods when details are shared between app users (refer to information on random user IDs)

Other privacy notices

Privacy notices relating to other parts of the NHS Test and Trace Programme:

- testing privacy potice (https://www.gov.uk/government/publications/coronavirus-covid-19-testing-privacy-information/testing-for-coronavirus-privacy-information)
- contact tracing privacy notice (https://contact-tracing.phe.gov.uk/help/privacy-notice)
- PHE COVID-19 privacy information (https://www.gov.uk/government/publications/phe-privacy-information/covid-19-privacy-information)
- venue logs (https://www.gov.uk/guidance/maintaining-records-of-staff-customers-and-visitors-to-support-nhs-test-and-trace)