



Article 9(2)(h) of UK GDPR, plus Schedule 1, Part 1, Paragraph 2 “Health or social care purposes” of DPA 2018.

The NOA and NHSE will share this data with

We treat the data we hold with great care. All data which is shared by NHS England is subject to robust rules relating to privacy, security and confidentiality and only the minimum amount of data necessary to achieve the relevant health and social care purpose will ever be shared.

Data is shared or is expected to be shared with organisations such as healthcare providers, clinicians, and commissioners of NHS services, for example:

- **the organisation that provided your care:** to assess the effectiveness of your care and to improve the services they offer
- **The Department of Health and Social Care:** to inform policy and guidelines
- **organisations responsible for the commissioning of NHS services in England, such as Integrated Care Boards:** to plan and improve weight management services and for benchmarking
- **local authorities:** to help plan and improve weight management services
- **research organisations, including universities and charities:** to carry out research

These organisations must apply for access to NOA data through NHS England’s [Data Access Request Service](#). Each application is assessed very carefully to make sure that the organisation:

- has a legal basis to access the data for that purpose
- will use the data for the benefit of health and care and for the agreed purposes only
- will handle and store the data securely

We only share data which can identify you (identifiable data) if this is absolutely necessary and the organisation who has made an application for data cannot achieve their purpose without it. Where possible we remove information from the data which identifies you, or we replace it with a unique reference number (this is known as pseudonymisation).

Each organisation we share data with must sign a [Data Sharing Framework Contract](#) and a [Data Sharing Agreement](#) and we carry out [audits](#) to check they are using the data as agreed.

Details about the NOA data we have shared with other organisations, except for anonymous data, will be published in the [NHS England Data Uses Register](#).

Practice Third party processors

In order to deliver the best possible service, the practice will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition, the practice will use carefully selected third party service providers. When we use a third party service provider to process data on our behalf then we will always have an appropriate agreement in



Data Protection Requirements. Our policy is to ensure all personal data related to our patients will be protected.

All employees and sub-contractors engaged by our practice are asked to sign a confidentiality agreement. The practice will, if required, sign a separate confidentiality agreement if the client deems it necessary. If a sub-contractor acts as a data processor for Wootton Medical Centre an appropriate contract (art 24-28) will be established for the processing of your information.

In certain circumstances you may have the right to withdraw your consent to the processing of data. Please contact the Data Protection Officer in writing if you wish to withdraw your consent. In some circumstances we may need to store your data after your consent has been withdrawn to comply with a legislative requirement.

Some of this information will be held centrally and used for statistical purposes. Where we do this, we take strict measures to ensure that individual patients cannot be identified. Sometimes your information may be requested to be used for research purposes – the surgery will always gain your consent before releasing the information for this purpose in an identifiable format. In some circumstances you can Opt-out of the surgery sharing any of your information for research purposes.

With your consent we would also like to use your information

There are times that we may want to use your information to contact you or offer you services, not directly about your healthcare, in these instances we will always gain your consent to contact you. We would however like to use your name, contact details and email address to inform you of other services that may benefit you. We will only do this with your consent. There may be occasions where authorised research facilities would like you to take part on innovations, research, improving services or identifying trends, you will be asked to opt into such programmes if you are happy to do so.

At any stage where we would like to use your data for anything other than the specified purposes and where there is no lawful requirement for us to share or process your data, we will ensure that you have the ability to consent and opt out prior to any data processing taking place.

This information is not shared with third parties or used for any marketing and you can unsubscribe at any time via phone, email or by informing the practice DPO as below.



NHS Digital Data Collection from the Practice

The NHS needs data about the patients it treats to plan and deliver its services and to ensure that care and treatment provided is safe and effective. The General Practice Data for Planning and Research data collection will help the NHS to improve health and care services for everyone by collecting patient data that can be used to do this. For example patient data can help the NHS to:

- monitor the long-term safety and effectiveness of care
- plan how to deliver better health and care services
- prevent the spread of infectious diseases
- identify new treatments and medicines through health research

GP practices already share patient data for these purposes, but this new data collection will be more efficient and effective.

This means that GPs can get on with looking after their patients, and NHS Digital can provide controlled access to patient data to the NHS and other organisations who need to use it, to improve health and care for everyone.

Contributing to research projects will benefit us all as better and safer treatments are introduced more quickly and effectively without compromising your privacy and confidentiality.

NHS Digital has engaged with the [British Medical Association \(BMA\)](#), [Royal College of GPs \(RCGP\)](#) and the [National Data Guardian \(NDG\)](#) to ensure relevant safeguards are in place for patients and GP practices.

NHS Digital purposes for processing patient data

Patient data from GP medical records kept by GP practices in England is used every day to improve health, care and services through planning and research, helping to find better treatments and improve patient care. The NHS is introducing an improved way to share this information - called the General Practice Data for Planning and Research data collection.

NHS Digital will collect, analyse, publish and share this patient data to improve health and care services for everyone. This includes:

- informing and developing health and social care policy
- planning and commissioning health and care services
- taking steps to protect public health (including managing and monitoring the coronavirus pandemic)
- in exceptional circumstances, providing you with individual care
- enabling healthcare and scientific research

Any data that NHS Digital collects will only be used for health and care purposes. It is never shared with marketing or insurance companies.

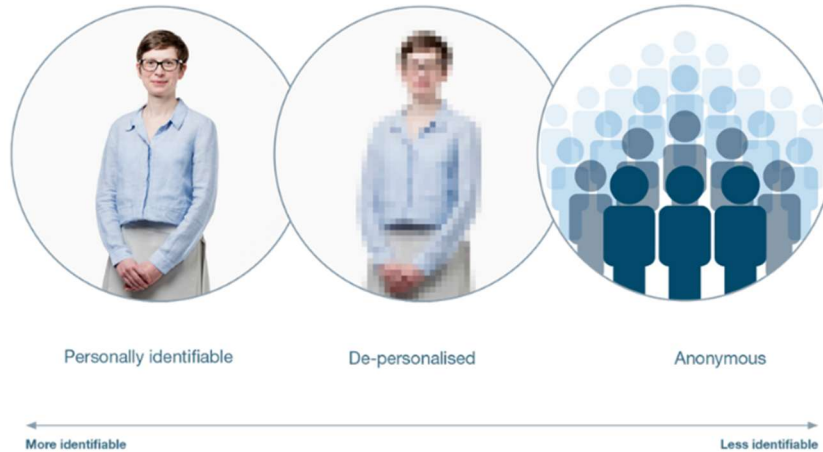


Image provided by Understanding Patient Data [under licence](#).

NHS Digital will be able to use the same software to convert the unique codes back to data that could directly identify you in certain circumstances, and where there is a valid legal reason. Only NHS Digital has the ability to do this. This would mean that the data became personally identifiable data in the diagram above. An example would be where you consent to your identifiable data being shared with a research project or clinical trial in which you are participating, as they need to know the data is about you.

More information about when we may be able to re-identify the data is in the [who we share your patient data with](#) section below.

The NHS Digital programme will be providing further information as the programme progresses. In the meantime, if you have any questions, you can contact the programme at enquiries@nhsdigital.nhs.uk.

The NHS Digital web pages also provide further information at <https://digital.nhs.uk/data-and-information/data-collections-and-data-sets/data-collections/general-practice-data-for-planning-and-research#additional-information-for-gp-practices>.

The Data NHD Digital collect

We will only collect structured and coded data from patient medical records that is needed for specific health and social care purposes explained above.

Data that directly identifies you as an individual patient, including your NHS number, General Practice Local Patient Number, full postcode, date of birth and if relevant date of death, is replaced with unique codes produced by de-identification software before it is sent to NHS Digital. This means that no one will be able to directly identify you in the data.

NHS Digital will be able to use the software to convert the unique codes back to data that could directly identify you in certain circumstances, and where there is a valid legal reason.



If you wish to register a Type 1 Opt-out with your GP practice before data sharing starts with NHS Digital, this should be done by returning this form to your GP practice. If you have previously registered a Type 1 Opt-out and you would like to withdraw this, you can also use the form to do this. You can send the form by post or email to your GP practice or call 0300 3035678 for a form to be sent out to you.

If you register a Type 1 Opt-out after your patient data has already been shared with NHS Digital, no more of your data will be shared with NHS Digital. NHS Digital will however still hold the patient data which was shared with us before you registered the Type 1 Opt-out.

If you do not want NHS Digital to share your identifiable patient data (personally identifiable data in the diagram above) with anyone else for purposes beyond your own care, then you can also register a National Data Opt-out. There is more about National Data Opt-outs and when they apply in the National Data Opt-out section below.

NHS Digital legal basis for collecting, analysing and sharing patient data.

When we collect, analyse, publish and share patient data, there are strict laws in place that we must follow. Under the UK General Data Protection Regulation (GDPR), this includes explaining to you what legal provisions apply under GDPR that allows us to process patient data. The GDPR protects everyone's data.

NHS Digital has been directed by the Secretary of State for Health and Social Care under the General Practice Data for Planning and Research Directions 2021 to collect and analyse data from GP practices for health and social care purposes including policy, planning, commissioning, public health and research purposes.

NHS Digital is the controller of the patient data collected and analysed under the GDPR jointly with the Secretary of State for Health and Social Care.

All GP practices in England are legally required to share data with NHS Digital for this purpose under the Health and Social Care Act 2012 (2012 Act). More information about this requirement is contained in the Data Provision Notice issued by NHS Digital to GP practices.

NHS Digital has various powers to publish anonymous statistical data and to share patient data under sections 260 and 261 of the 2012 Act. It also has powers to share data under other Acts, for example the Statistics and Registration Service Act 2007.

Regulation 3 of the Health Service (Control of Patient Information) Regulations 2002 (COPI) also allow confidential patient information to be used and shared appropriately and lawfully in a public health emergency. The Secretary of State has issued legal notices under COPI (COPI Notices) requiring NHS Digital, NHS England and Improvement, arm's-length bodies (such as Public Health England), local authorities, NHS trusts, Integrated Care Boards and GP practices to share confidential patient information to respond to the COVID-19 outbreak. Any information used or shared during the COVID-19 outbreak will be limited to the period of the outbreak unless there is another legal basis to use confidential patient information.

The legal basis under UKGDPR for General Practice Data for Planning and Research



- primary care networks (PCNs), Integrated Care Boards (ICBs) and integrated care organisations (ICOs)
- local authorities
- research organisations, including universities, charities, clinical research organisations that run clinical trials and pharmaceutical companies

If the request is approved, the data will either be made available within a secure data access environment within NHS Digital infrastructure, or where the needs of the recipient cannot be met this way, as a direct dissemination of data. We plan to reduce the amount of data being processed outside central, secure data environments and increase the data we make available to be accessed via our secure data access environment. For more information read about improved data access in [improving our data processing services](#).

Data will always be shared in the uniquely coded form (de-personalised data in the diagram above) unless in the circumstances of any specific request it is necessary for it to be provided in an identifiable form (personally identifiable data in the diagram above). For example, when express patient consent has been given to a researcher to link patient data from the General Practice for Planning and Research collection to data the researcher has already obtained from the patient.

It is therefore possible for NHS Digital to convert the unique codes back to data that could directly identify you in certain circumstances, and where there is a valid legal reason which permits this without breaching the common law duty of confidentiality. This would include:

- where the data was needed by a health professional for your own care and treatment
- where you have expressly consented to this, for example to participate in a clinical trial
- where there is a legal obligation, for example where the COPI Notices apply - see [Our legal basis for collecting, analysing and sharing patient data](#) above for more information on this
- where approval has been provided by the [Health Research Authority](#) or the Secretary of State with support from the [Confidentiality Advisory Group \(CAG\)](#) under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 (COPI) - this is sometimes known as a 'section 251 approval'

This would mean that the data was personally identifiable in the diagram above. Re-identification of the data would only take place following approval of the specific request through the Data Access Request Service, and subject to independent assurance by IGARD and consultation with the Professional Advisory Group, which is made up of representatives from the BMA and the RCGP. If you have registered a National Data Opt-out, this would be applied in accordance with the National Data Opt-out policy before any identifiable patient data (personally identifiable data in the diagram above) about you was shared. More about the National Data Opt-out is in the section below.

Details of who we have shared data with, in what form and for what purposes are published on our [data release register](#).



You will be informed who your data will be shared with and in some cases asked for consent for this to happen when this is required.

Computer System

This practice operates a Clinical Computer System on which NHS Staff record information securely. This information can then be shared with other clinicians so that everyone caring for you is fully informed about your medical history, including allergies and medication.

To provide around the clock safe care, unless you have asked us not to, we will make information available to our Partner Organisation (above). Wherever possible, their staff will ask your consent before your information is viewed.

Shared Care Records

To support your care and improve the sharing of relevant information to our partner organisations (as above) when they are involved in looking after you, we will share information to other systems. You can opt out of this sharing of your records with our partners at any time if this sharing is based on your consent.

We may also use external companies to process personal information, such as for archiving purposes. These companies are bound by contractual agreements to ensure information is kept confidential and secure. All employees and sub-contractors engaged by our practice are asked to sign a confidentiality agreement. If a sub-contractor acts as a data processor for Wootton Medical Centre an appropriate contract (art 24-28) will be established for the processing of your information.

Sharing your information without consent

We will normally ask you for your consent, but there are times when we may be required by law to share your information without your consent, for example:

- where there is a serious risk of harm or abuse to you or other people;
- Safeguarding matters and investigations
- where a serious crime, such as assault, is being investigated or where it could be prevented;
- notification of new births;
- where we encounter infectious diseases that may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS);
- where a formal court order has been issued;
- where there is a legal requirement, for example if you had committed a Road Traffic Offence.

How long will we store your information?

We are required under UK law to keep your information and data for the full retention



- Moulton Surgery
- Woodview Medical Centre
- Denton Village Surgery
- Kingsthorpe Medical Centre

Primary Care Networks form a key building block of the NHS long-term plan. Bringing general practices together to work at scale has been a policy priority for some years for a range of reasons, including improving the ability of practices to recruit and retain staff; to manage financial and estates pressures; to provide a wider range of services to patients and to more easily integrate with the wider health and care system.

This means the practice may share your information with other practices within the PCN to provide you with your care and treatment.

Service Evaluation

The PCN carries out service evaluations to improve the quality and accessibility of primary care services. This may be carried out in several ways including telephone surveys, online surveys and interviews.

The legal basis for contacting you to take part -

Article 6, e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;”

Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems

To process the survey information, we collect from you we will only do so with your consent.

Article 6(1)(a) - Consent of the data subject (you)

Article 9(2)(a) – Explicit consent of the data subject. (you)’

Population Health Management

Population Health Management (or PHM for short) is aimed at improving the health of an entire population. The PHM approach requires health care organisations to work together with communities and partner agencies, for example, GP practices, community service providers, hospitals and other health and social care providers. These organisations will share and combine information with each other in order to get a view of health and services for the population in a particular area. This information sharing is subject to robust security arrangements.



contact details (such as your mobile phone number), the practice will from time to time ask you to confirm that the information we currently hold is accurate and up-to-date.

Online Access

You may ask us if you wish to have online access to your medical record. However, there will be certain protocols that we have to follow to give you online access, including written consent and the production of documents that prove your identity.

Please note that when we give you online access, the responsibility is yours to make sure that you keep your information safe and secure if you do not wish any third party to gain access.

Third parties mentioned on your medical record

Sometimes we record information about third parties mentioned by you to us during any consultation, or contained in letters we receive from other organisations. We are under an obligation to make sure we also protect that third party's rights as an individual and to ensure that references to them which may breach their rights to confidentiality, are removed before we send any information to any other party including yourself.

The NHS wants to give people better ways to see their personal health information online. We know that people want to be able to access their health records. It can help you see test results faster. It also lets you read and review notes from your appointments in your own time.

From 01/11/2022 we're now letting you see all the information within your health record automatically. If you are over 16 and have an online account, such as through the [NHS App](#), [NHS website](#), or another online primary care service, you will now be able to see all future notes and health records from your doctor (GP). Some people can already access this feature, this won't change for you.

This means that you will be able to see notes from your appointments, as well as test results and any letters that are saved on your records. This only applies to records from your doctor (GP), not from hospitals or other specialists. You will only be able to see information from the date of registration. For most people, access will be automatic, and you won't need to do anything.

Your doctor (GP) may talk to you to discuss test results before you are able to see some of your information on the app. Your doctor (GP) may also talk to you before your full records access is given to make sure that having access is of benefit to you. There might be some sensitive information on your record, so you should talk to your doctor if you have any concerns.

These changes only apply to people with online accounts. If you do not want an online account, you can still access your health records by requesting this information through reception. The changes also only apply to personal information about you. If you are a carer and would like to see information about someone you care for, speak to reception staff.



About the NHS OpenSAFELY Data Analytics Service pilot

The NHS OpenSAFELY Data Analytics Service is a secure data analytics service managed by NHS England. It is available to approved users (such as academics, data analysts, data scientists and researchers) to help them to analyse patient data which is held by your GP practice and by NHS England, in a safe and secure way that protects your privacy.

This is a pilot service which builds upon the success of the NHS England OpenSAFELY COVID-19 Service, which was introduced to:

- help identify medical conditions and medications which affect the risk or impact of COVID-19 infection on individuals
- identify the risk factors associated with poor patient outcomes
- gather information to monitor and predict the demand on health services

The service uses a software platform called OpenSAFELY which is designed with the following privacy safeguards:

OpenSAFELY uses pseudonymised data, held by your GP practice and by NHS England. Pseudonymised data is where information which can uniquely identify you, such as your NHS number, is replaced with a unique marker (a random string of letters and numbers). Other information which can also uniquely identify you, such as your name, date of birth and address are also removed from the data and replaced with something more general, for example, your date of birth is replaced with your age and your postcode is replaced with a geographical region. More information about pseudonymisation and other techniques used to protect your privacy can be found on the Understanding Patient Data website.

The OpenSAFELY software does not move patient data outside of the secure IT environments they are held in. Instead, the software is implemented inside the data centres of the 2 largest GP IT system suppliers, TPP and Optum so that when approved users of OpenSAFELY run code to analyse the pseudonymised data, it never leaves your GP practice's IT system.

Approved users are given access to an off-line development environment, where they can build and develop their data analysis code using 'dummy' (pretend or fictional) data rather than real patient data. The code is tested before it is sent securely into the live data environment to be executed (run) against the real pseudonymised patient data held in your GP practice's IT system. This means that approved users never see any real patient data, cannot download any real patient data and can only see aggregate anonymous results or outputs (which do not identify you).

A record (a log) is kept of all user activity and code which has been executed on the OpenSAFELY software platform and is published.



Approved users who are conducting approved data analytic projects on pseudonymised data within the service (such as academics, data analysts, data scientists and researchers) will only see aggregate anonymous results and outputs (which do not identify you). A summary of the projects which have been given approval are published.

Our data processors

Under a Data Processing Agreement (contract), NHS England has instructed:

- the Phoenix Partnership (Leeds) Ltd (TPP) and Optum (formerly EMIS Group PLC) to host the service in their secure data centres and allow access to approved users
 - the Bennett Institute for Applied Data Science (University of Oxford) to provide platform development functions and conduct analyses of the data held on the service
-

How long data is kept

Your data will be kept for as long as is necessary to deliver and run the service in accordance with the NHS Records Management Code of Practice 2021, NHS England's Records Management Policy and the UK GDPR and the Data Protection Act 2018.

The aggregate anonymous results and outputs made available to approved users of the service will be kept in line with the above policies to check and validate the data analysis and for audit purposes.

Where we store the data

The OpenSAFELY secure platform stores and processes data in the UK.

Our legal basis and role

Data protection law requires NHS England to have a legal basis before we can process your personal data.

Our legal basis is:



You can make register a Type 1 opt-out by completing a form and returning it to your GP practice. More information is available on the NHS website.

National Data Opt-Out

The National Data Opt-Out allows patients to opt out of their confidential patient information being used for research or planning purposes. If you have registered a National Data Opt-Out, your data will still be processed by NHS OpenSAFELY Data Analytics Service, with certain exceptions*. This is because the National Data Opt-Out does not apply where NHS England has a legal obligation to operate the service under the NHS OpenSAFELY Data Analytics Service Pilot Directions 2025. The National Data Opt-Out also does not apply to aggregate anonymous data (data which does not identify you) which is the only data shared with approved users of the OpenSAFELY service.

Data Protection Officer For NHSE Pilot

We take our responsibility to look after your data very seriously. If you have any questions or concerns about how NHS England uses your data, please contact our Data Protection Officer at: england.dpo@nhs.net.

You also have the right to make a complaint about how we are using your data to the Information Commissioner's Office by calling 0303 123 1113 or through the [ICO website](#).

Changes to this notice

This privacy notice was first published on 22 July 2025. NHS England may make changes to this privacy notice. If so, the date it was last amended will be shown below. Changes to this notice will apply immediately from the date of any change.

Medical Examiner Service

Following the death of any patients of Wootton Medical Centre we are now obliged to inform NHS Trust, Medical Examiner Service.

Medical examiner offices at acute trusts now provide independent scrutiny of non-coronial deaths occurring in acute hospitals. The role of these offices is now being extended to also cover deaths occurring in the community.

Medical examiner offices are led by medical examiners, senior doctors from a range of specialties including general practice, who provide independent scrutiny of deaths not taken



If you would like to know more about your rights in respect of the personal data we hold about you, please contact the Data Protection Officer as below.

Data Protection Officer:

The Practice Data Protection Officer is Paul Couldrey of PCIG Consulting Limited. Any queries regarding Data Protection issues should be addressed to him at: -

Email: info@pcdc.org.uk

Postal: PCIG Consulting Limited

7 Westacre Drive

Quarry Bank

Dudley

West Midlands

DY5 2EE

Changes:

It is important to point out that we may amend this Privacy Notice from time to time. If you are dissatisfied with any aspect of our Privacy Notice, please contact the Practice Data Protection Officer.