Classification: Official

NHS England privacy notice

Version: 1.7070

What is a Privacy Notice?

Find out about privacy notices and what they should include.

The UK General Data Protection Regulation (GDPR) requires that data controllers provide certain information to people whose information (personal data) they hold and use. A privacy notice is one way of providing this information. This is sometimes referred to as a fair processing notice.

A privacy notice should identify who the data controller is, with contact details for its Data Protection Officer. It should also explain the purposes for which personal data are collected and used, how the data are used and disclosed, how long it is kept, and the controller's legal basis for processing.

NHS England's privacy notice is set out in the following pages.

NHS England as a Data Controller

Details of our data protection responsibilities and how to contact us.

NHS England is a data controller under the UK General Data Protection Regulation (GDPR) and the Data Protection Act (DPA) 2018. Our head office address is:

NHS England London
Skipton House
80 London Road
London
SE1 6LH

How to contact us

Please contact us if you have any questions about our privacy notice or information we hold about you:

Customer Contact Centre
Telephone: 0300 311 22 33
Email: england.contactus@nhs.net
Post: NHS England, PO Box 16738, Redditch, B97 9PT

Our opening hours are: 8am to 6pm Monday to Friday, except Wednesdays when we open at the later time of 9.30am.

Contact details of our Data Protection Officer

NHS England have appointed a Data Protection Officer (DPO). If you have any queries about this privacy notice or about how NHS England process personal data please contact our DPO at the address below.

Jon Moore (interim DPO)
Delivery Directorate
NHS England
Quarry House
Quarry Hill
Leeds
LS2 7UE
E-mail: england.dpo@nhs.net

The role of the Data Protection Officer

As a public authority, NHS England are required to appoint a data protection officer (DPO). This is an essential role in facilitating 'accountability', and the organisations' ability to demonstrate compliance with the GDPR. The essential qualities of the role are to provide support, advice and assurance of all our activities that involve processing personal data. The DPO reports on compliance to our senior management teams and is empowered to raise data protection matters with our Board if necessary.

The DPO has expert knowledge of data protection law and practices, and a detailed understanding of how NHS England processes personal data.

NHS England have a comprehensive suite of policies and procedures that addresses all aspects of information governance and data protection. These govern how we ensure that the personal data we are responsible is processed and shared lawfully, and that peoples' data protection rights are respected.

NHS England's legal basis for processing personal data

NHS England is a public body established by the NHS Act 2006 as amended by the Health and Social Care Act 2012. As such our business is based upon statutory powers which underpin the legal bases that apply for the purposes of the GDPR. The legal bases for the majority of our processing is:

> Article 6(1)(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.

For entering into and managing contracts with the individuals concerned, for example our employees the legal basis is:

> Article 6(1)(b) – processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

Where we have a specific legal obligation that requires the processing of personal data, the legal basis is:

Article 6(1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject.

Where we process special categories data, for example data concerning including health, racial or ethnic origin, or sexual orientation, we need to meet an additional condition in the GDPR. Where we are processing special categories personal data for purposes related to the commissioning and provision of health services the condition is:

Article 9(2)(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 and services…

Where we process special categories data for employment or safeguarding purposes the condition is:

Article 9(2)(b) – processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law…

NHS England may also process personal data for the purpose of, or in connection with, legal proceedings (including prospective legal proceedings), for the purpose of obtaining legal advice, or for the purpose of establishing, exercising or defending legal rights. Where we process personal data for these purposes, the legal basis for doing so is:

Article 6(1)(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; or

Article 6(1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject; or

Article 6(1)(f) – processing is necessary for the purposes of legitimate interests pursued by the controller.

Where we process special categories of personal data for these purposes, the legal basis for doing so is:

Article 9(2)(f) – processing is necessary for the establishment, exercise or defence of legal claims; or

Article 9(2)(g) – processing is necessary for reasons of substantial public interest.

In How we use your information we set out most of the key ways in which we may process your personal data for the purposes of, or in connection with our statutory functions. If you want to know more about how we process your data please contact our Customer Contact Centre.

How long do we keep information about you?

You can obtain a copy of our Corporate Records Retention and Disposal Schedule, and Primary Care Services Retention Schedule from our Privacy Notice web site, or by contacting our Customer Contact Centre. We also comply with the Records Management Code of Practice for Health and Social Care published by the Information Governance Alliance.

Your rights

The GDPR includes a number of rights that are more extensive that those in the Data Protection Act 1998. We must generally respond to requests in relation to your rights within one month, although there are some exceptions to this.

The availability of some of these rights depends on the legal basis that applies in relation to the processing of your personal data, and there are some other circumstances in which we may not uphold a request to exercise a right. Your rights and how they apply are described below.

Right to be informed

Your right to be informed is met by the provision of this privacy notice, and similar information when we communicate with you directly – at the point of contact.

Right of access

You have the right to obtain a copy of personal data that we hold about you and other information specified in the GDPR, although there are exceptions to what we are obliged to disclose.

A situation in which we may not provide all the information is where in the opinion of an appropriate health professional disclosure would be likely to cause serious harm to your, or somebody else's physical or mental health.

Right to rectification

You have the right to ask us to rectify any inaccurate data that we hold about you.

Right to erasure (‘right to be forgotten’)

You have the right to request that we erase personal data about you that we hold. This is not an absolute right, and depending on the legal basis that applies, we may have overriding legitimate grounds to continue to process the data.

Right to restriction of processing

You have the right to request that we restrict processing of personal data about you that we hold. You can ask us to do this for example where you contest the accuracy of the data.

Right to data portability

This right is only available where the legal basis for processing under the GDPR is consent, or for the purposes of a contract between you and NHS England. For this to apply the data must be held in electronic form. The right is to be provided with the data in a commonly used electronic format.

Right to object

You have the right to object to processing of personal data about you on grounds relating to your particular situation. The right is not absolute and we may continue to use the data if we can demonstrate compelling legitimate grounds.

Rights in relation to automated individual decision-making including profiling

You have the right to object to being subject to a decision based solely on automated processing, including profiling. Should we perform any automated decision-making, we will record this in our privacy notice, and ensure that you have an opportunity to request that the decision involves personal consideration.

Right to complain to the Information Commissioner

You have the right to complain to the Information Commissioner if you are not happy with any aspect of NHS England’s processing of personal data or believe that we are not meeting our responsibilities as a data controller. The contact details for the Information Commissioner are:

Information Commissioner’s Office
Wycliffe House
Water Lane,
Wilmslow
SK9 5AF
ico.org.uk
0303 123 1113

How to access your personal information

How to make a request for personal data that we hold about you and how to make a request about your other data protection rights.

Medical records

Find out how to get a copy of your medical records

Information held by NHS England

Requests may be made in writing, by email, or by speaking to us – see NHS England » NHS England as a data controller

All requests will be recorded, and you may need to provide information to verify your identity and enable us to locate the information. Please provide:

- Full name, address, date of birth, NHS number (requests for health records only)
- An indication of what information you are requesting to enable us to locate this in an efficient manner.

Examples of acceptable identity evidence are listed below. We require, where applicable, two items from List A and one from List B

List A: ID documents, examples are -

- Birth certificate
- Passport
- Driving license
- Staff ID badge (for NHS England employees only)

List B: Proof of Address, examples are -

- Bank statement
- Utility bill
- Tax certificate

National Vaccination Programmes

How we use personal data to support the National Vaccination Programmes

NHS England (NHSE) has been given responsibility by the Secretary of State, for the delivery of a number of Vaccination Programmes provided by the NHS for England.

Information about the types of vaccinations that are available in the UK, those provided by the NHS and also when to have them can be found here – Vaccinations - NHS (www.nhs.uk).

NHSE is supported by a number of different agencies and other health organisations in order to deliver the different programmes.

This transparency notice provides information about the programmes where NHSE is providing a centralised national approach to any of the activities listed below:

- The selection of citizens eligible for a particular vaccination
- Inviting eligible citizens for their vaccination
- Enabling citizens to book an appointment to receive their vaccine
- Monitoring and managing the delivery, efficacy and safety of immunisation programmes including adverse reactions to vaccines and medicines

Purposes for which we process your data

We will collect, process, and disseminate citizen data to:

- Identify people who we are advised are eligible for a particular vaccination in line with the guidance provided by the Joint Committee on Vaccination and Immunisation. Further details of their work can be found at – Joint Committee on Vaccination and Immunisation - GOV.UK (www.gov.uk)
- Send you national invitations where we feel that this will be of benefit to you
- Support GP's and other vaccination providers to contact you to tell you about any vaccination that you are eligible for
- Enable you to book your vaccination
- Send you reminders that encourage you to book a vaccination where they are needed
- Send your vaccination information to your GP electronically, if you are registered to an English GP practice
- Ensure that you can access a vaccination at a suitable location and that there is vaccination available to give to you
- Check that people are receiving their vaccinations as we expect so that we can take measures to support our vaccination providers in areas of low uptake. In these cases, we do not need to know who you are, so we ask for the data to be altered so that your name and address is not visible to anyone apart from those responsible for your care
- Provide reports to support planning for the current and future vaccination programmes
- Support incorrect vaccination records to be corrected where this is possible
- Provide systems to enable vaccination providers to record a vaccination and for that data to flow to us and onwards to GP records. How to use the service - NHS Record a vaccination (england.nhs.uk) for further information

- Ensure that systems used to record your vaccination are able to display your immunisation history to help clinicians
- Enable you to view a full record of your vaccination history through your GP records or the NHS APP
- Provide data to the UK Health Security Agency – see UK Health Security Agency - GOV.UK (www.gov.uk) so that they can carry out their duties to protect the health of the population
- Provide data to the NHS Business Services Authority – see Welcome | NHSBSA so that they can help us manage claims for payment from vaccination service providers and to ensure that any discrepancies are highlighted and dealt with appropriately

The controller of your personal data

Under the UK General Data Protection Regulation 2016 (UK GDPR), NHS England is the controller of your personal data where we process it for national vaccination programme purposes. Our legal basis is set out in the table below:

1) Compliance with an Article 6 condition in the UK GDPR
The processing that we undertake complies with condition 6(1)(e), which applies where processing is necessary for the performance of a task carried out in the public interest. This task has to be set out in UK domestic law. The relevant UK law is section 8 of the Data Protection Act 2018 ("DPA 2018"). This states that the section 6(1)(e) condition is met if the processing of personal data is necessary for the exercise of a "function" given to a public body by legislation. A function is a task or duty that the legislation says the public may or must perform. Under the *NHS public health functions agreement 2023 to 2024 - GOV.UK (www.gov.uk)* (and all previous and future versions of the agreement) the Secretary of State arranges for certain elements of their public health functions to be exercised by NHS England. The Secretary of State is able to make such arrangements with NHS England under section 7A of the National Health Service Act 2006 (**"the 2006 Act"**). We will therefore refer to this agreement as **"the 7A Agreement"**. The overarching functions that we are exercising on behalf of the Secretary of State are set out in the "Legal framework" section of the Agreement. Sections 2A and 2B

of the 2006 Act relate to the protection or improvement of public health. Section 2A describes the steps that may be taken by the Secretary of State under that section which includes providing vaccination, immunisation or screening services.

The particular tasks that we must carry out to assist with the exercise of these functions are set out in Annex A of the 7A Agreement which lists the vaccination and immunisations programmes to be provided.

2) Compliance with an Article 9 condition in the UK GDPR

As the data used includes special category data a Schedule 9 condition must be complied with.

a) Health and social care purposes - Article 9(2)(h)

The processing complies with condition 9(2)(h), which applies if the processing is necessary for the purposes of preventive medicine, the provision of health or social care or treatment or the management of health or social care systems and services, as further detailed in UK law.

The relevant UK law is section 10(2) and paragraph 2 of Schedule 1 of the Data Protection Act 2018. Paragraph 2 confirms that Article 9(2)(h) covers processing necessary for preventive medicine, the provision of health care and the management of health care systems. These points cover all processing of personal data carried out as part of the immunisation programmes.

b) Public health – Article 9(2)(i)

The processing also complies with Article 9(2)(i), which applies if the processing is necessary for reasons of public interest in the area of public health, as further detailed in UK law.

The relevant UK law is section 10(2) and paragraph 3 of Schedule 1 of the Data Protection Act 2018. Paragraph 3 confirms that Article 9(2)(i) covers processing carried out in the public interest in the area of public health and under the responsibility of a health professional.

3) Compliance with the common law duty of confidentiality (CLDC)

The Health Service (Control of Patient Information) Regulations 2002 (**"COPI Regulations"**) were passed to ensure that there was clear authority for the processing of confidential patient information in certain circumstances. They suspend the duty of confidentiality where confidential patient information is being processed in the circumstances described in the Regulations.

Regulation 3 says that confidential patient information may be "processed" with a view to:

- recognising trends in communicable diseases and other risks to public health
- monitoring and managing:
    - outbreaks of communicable disease
    - the delivery, efficacy and safety of immunisation programmes
    - adverse reactions to vaccines and medicines
    - providing information to people about the risks of acquiring communicable diseases

"Processing" includes obtaining patient information, using it and disclosing it to other organisations. It also includes maintaining any databases containing patient information that are necessary for the purposes set out above.

The use of patient data for the programme falls within the tasks described in the Regulation and the definition of “processing”.

COVID-19 and Seasonal Influenza

To support the healthcare response to COVID-19, NHS England is directed under the COVID-19 Public Health Directions 2020, 17th March 2020 (as amended) to:

- establish information systems to collect and analyse data in connection with COVID-19; and
- develop and operate IT systems to deliver services in connection with COVID-19

Where we are directed to process personal data for COVID-19 purposes, this is a legal obligation, and we are required to do this under Article 6 (1)(c) of UK GDPR.

We also rely on this Direction to process data for seasonal influenza immunisation purposes. For further information on how we collect and process data for COVID-19 and seasonal flu vaccination programmes see COVID-19 At Risk Patients - NHS England Digital

We are also allowed to share your personal data under UK GDPR where it is necessary for us to do so.

Types of personal data we currently process which will vary dependent on the vaccination programme) NOTE - this will be updated when additional vaccination programme data processing requirements are finalised)

	Programme						
Data Item	COVID-19	Flu	MMR[1]	HPV[2]	RSV[3]		Pertussis[4]
					Maternity	Older Persons	
NHS number	Yes	Yes	Yes	Yes	Yes	Yes	Yes
names	Yes	Yes	Yes	Yes	Yes	Yes	Yes
gender	Yes	Yes	Yes	Yes	Yes	Yes	Yes
date of birth	Yes	Yes	Yes	Yes	Yes	Yes	Yes
address	Yes	Yes	Yes	No	No	Yes	No
postcode	Yes	Yes	Yes	Yes	Yes	Yes	Yes
contact details such as an email address and mobile phone number	Yes	Yes	Yes	Yes	No	Yes	No
health related data in the form of condition codes held in central NHS records such as those held by your GP or a hospital where you have received healthcare	Yes	Yes	No	No	No	No	No
information about vaccinations received and details of any adverse reactions/doses/date/batch/type/body site/how administered/	Yes	Yes	Yes	Yes	Yes	Yes	Yes
if you are a Carer	Yes	Yes	No	No	No	No	No
if you are a Social care worker	Yes	Yes	No	No	No	No	No
if you are a Health care worker	Yes	Yes	No	No	No	No	No
if you are a Care home worker	Yes	Yes	No	No	No	No	No
if you are a Care home resident along with details of your care home	Yes	Yes	No	No	No	Yes	No
Ethnic category	Yes	Yes	Yes	No	Yes	Yes	Yes
Vaccination location (site code)	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[1] MMR – Measles, Mumps and Rubella vaccination
[2] HPV – Human Papilloma Virus vaccination
[3] RSV - Respiratory Syncytial Virus vaccination – Maternity (Infant) and Older Persons
[4] Pertussis – Whooping Cough vaccination

Consent to treatment information where we hold this a) the vaccination type requires this, b) due to the closure of a service or c) where the system holding the information in its original form is no longer available	Yes	Yes	No	Yes	No	No	No
Details of the person administering the vaccine including job role	No	No	No	Yes	Yes	Yes	Yes
School Unique Reference Number (URN) for pupils included in the relevant Schools Census, obtained from the Department for Education (DfE) to enhance the datasets used for vaccination programme uptake monitoring	Yes	Yes	Yes	Yes	No	No	Yes
Number of weeks pregnant (gestational age/due date)	No	No	No	No	Yes	No	Yes

How we obtain your personal data

Identifying citizens for eligibility for a vaccination is carried out using data we collect or already hold. More information is provided here – Cohorting as a Service (CaaS).

We also collect information about the vaccinations provided at the point of care; this data flows from any system used to record when a vaccination is given. We can then ensure that we have up to date information about your vaccination history and flow that data to those responsible for your health care, your GP.

We have developed a point of care system to enable vaccinations administered in Maternity Services and Community Pharmacies to be captured so that they can be flowed to your GP record automatically. This record a vaccination service is known as RAVS. We currently use this system for COVID-19, Flu, RSV and Pertussis vaccination data capture and will extend its use for other vaccinations as part of our Vaccination and Immunisation Strategy. You can find additional information here: How to use the service - NHS Record a vaccination (england.nhs.uk)

We also obtain a limited amount of data from the Department for Education (DfE) for the purposes of linking a school reference number to a child where the vaccination programme identifies a requirement to monitor vaccination uptake by school. There is a Data Sharing Agreement in place where this is required, and all data is de-identified prior to it being made available for analytics purposes.

How we process your data

Once it is agreed that a vaccination programme must be offered, we will process the data necessary to manage and monitor the vaccination programme including where we support the programme by running a national invitation campaign. We use cohorting as a service to develop the cohorts that contain the data we need.

A vaccination event contributes to your clinical care and where we decide to send a national vaccination invitation this is considered as a Direct Care activity. We will send invitations using SMS text messages, e-mails, through the NHS App or where necessary, by letter. We use our NHS Notify service NHS Notify - NHS England Digital to undertake this part of the processing.

We will send information on who has been invited for a particular vaccination to our National Booking Service, but this may not apply to all vaccinations at present.

We will use NHSE Arden and GEM Commissioning Support Unit, to de-identify the data and then make it available to our analysts in our analytics platforms. They will then link datasets so that we can manage and monitor the programmes.

In order to monitor and manage our programmes, we need to understand the number of people that have been invited for a vaccine, so we have a baseline figure to work from. The data that is obtained from vaccination providers in relation to the vaccinations that they administer is then used to provide actual figures. In order to be able to report progress as accurately as possible, we need these two types of data.

Sharing your data

We receive and share relevant information with organisations who have responsibilities for delivering vaccinations or for monitoring their safety.

We will share personal, identifiable and clinical information with or receive vaccination information from:

GP's	We request extracts of vaccination event data from GP systems where the GP has provided the vaccination, or the GP record is used as the source of that vaccination event (see box below). We will flow the vaccination data from any organisation that has administered an NHS funded vaccination and entered it into an assured and approved point of care system (POC) including our own RAVS system. We will flow a vaccination event to your GP clinical record even though your GP may have provided

	your vaccination, they may have recorded it in a different IT system.
School Aged Immunisation Services, the Child Health Information Service, Maternity Services and Primary Care Networks	We also process vaccination data that has been shared between systems by providers of local vaccination and immunisation services. Whilst they may not share data directly with us, we will obtain it from GP clinical records once it has been sent by the originating system or provider.
Pharmacies	We will enable demographic data and vaccination history to be available to the pharmacy staff once you have decided to obtain your vaccination at a pharmacy and the pharmacy staff are administering your vaccination. It will be available through our own Advanced Programming Interface (API), - see API platform - NHS Digital for more information. They will use a point of care system to record your vaccination and this data will flow to us and on to your GP.
Other NHS, health, or social care organisations	We will enable demographic data and vaccination history to be available in the same way that we do for pharmacies where an organisation needs to know this information to care for you. Some NHS Trust hospitals administer vaccinations where they have been contracted to do so. We ask them to use an NHS England provided point of care system so that the vaccination they administer can flow to us and on to your GP. We also make the data available in the summary care record – see Summary Care Record - NHS Digital for further information.
The UK Health Security Agency (UKHSA)	We share data so that the UKHSA can fulfil their statutory Public Health duties – see Framework document between DHSC and the UK Health Security Agency - GOV.UK (www.gov.uk) This includes - Letter from Maggie Throup to Professor Dame Jenny Harries, UKHSA chief executive -

	GOV.UK (www.gov.uk) for more information about the role of the UKHSA.
The NHS Business Services Authority (BSA)	We share data with the BSA because we are permitted to do so as it is necessary for us both to exercise certain functions in relation to the running and management of the NHS. The legal basis for the processing of this data for the purpose stated is Article 6 (1) e, where, under the NHS Act 2006, Chapter A1, Section 13Z3, (e, and (f. Specific Directions relating to the functions of the NHS Business Services Authority are made in the NHS Counter Fraud Authority Directions, with Supplemental Directions to the NHS Business Services Authority (Awdurdod Gwasanaethau Busnes y GIG) 2017, schedule which includes intelligence, detection, and prevention functions (paragraph 5) and Investigation functions (paragraph 7). See – NHS Counter Fraud Authority and supplemental directions 2017 - GOV.UK (www.gov.uk) for further information. We tell them you have had a vaccination, when, where and who administered it. We tell them your NHS number and your date of birth. This enables them to consolidate claims for payment from vaccination providers and ensure that these claims are made accurately. Linking data in this way is the only way to achieve this obligation.
The National Crime Agency	Personal data will be shared with the National Crime Agency where this data is needed for law enforcement purposes and is for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

What else do we use your data for?

Data will be used for programme evaluation, planning, commissioning, and where approved, could be used for research purposes, including relevant clinical trials. Ultimately, we need to understand whether vaccinations are effective and contributing to the improved health of the population in a way that is equitable.

The data we use for these purposes does not identify you. We change your NHS number into a random selection of characters and remove names and addresses. The data containing the random characters is then made available to analysts who are able to link any data with the same characters in it, but they will not know who you are.

The majority of reporting uses data relating to a number of unidentified people that has been grouped together and we further minimise the risk of identifying anyone by removing data where the analysis indicates there are less than 10 people to whom the data could relate to.

Further information about how we did this during the COVID-19 pandemic is here: -NHS England » NHS COVID-19 Data Store. We use the same technology currently for processing data for other national vaccination programmes.

Where we use data Processors, we have contracts and agreements in place with them which means that they can only process your personal data on our instructions. Our Processors must also comply with stringent security requirements when processing your personal data on our behalf.

How long we keep your personal data for

We will retain your personal data for as long as is necessary for the purposes outlined above in accordance with the relevant – Records Management Code of Practice - NHS Transformation Directorate (england.nhs.uk) .

Other organisations with whom we share your personal data have obligations to keep it for no longer than is necessary for the purposes for which we have shared your personal data. Information about this will be provided in their transparency or privacy notices which are published on their websites.

Data relating to the COVID-19 pandemic

Due to legislation published to support the UK COVID-19 Public Inquiry (see – UK Covid-19 Inquiry (covid19.public-inquiry.uk) for further information), NHS England and other organisations who supported the services provided during the Pandemic, are legally obliged to retain data relating to the Pandemic until such time as the COVID Inquiry deems it is no longer necessary to retain it for their purposes. At that point in time, we will review retention periods to ensure that we are fulfilling our obligations under the Records Management Code of Practice and therefore expect our retention periods to be longer than stated in the Code.

Where we store the data

We store and process your personal data within the United Kingdom but where our Processors need to process your personal data outside of the UK, we will always ensure that the transfer outside of the UK complies with data protection laws.

Statistical data, which does not allow you to be identified, may be stored and processed outside of the UK.

Your rights over your personal data

To read more about the information we collect, our legal basis for collecting this information and what choices and rights you have, see – how we look after your health and care information.

As NHS England has now merged with NHS Digital and Health Education England, additional transparency information about the data we are now the Controller for can be found at

NHS England » NHS England's privacy notice

Transparency notice: how we use your personal data - NHS Digital

Privacy notice | Health Education England (hee.nhs.uk)

Type 1 opt outs and the National Data Opt Out

In most vaccination programmes, any Type 1 opt outs recorded within your GP record will not apply where the data obtained from GP systems is for a Direct Care purpose; we are obliged to monitor uptake of the vaccination which, although a secondary purpose, is linked to direct care.

The National Data Opt Out will not apply in all cases where any disclosure is for the purposes of monitoring and control of communicable disease or other risks to public health which includes:

- diagnosing communicable diseases
- controlling or preventing their spread
- delivering and monitoring vaccination programmes

Where processing is in relation to planning and research, we will adhere to the National Data Opt Out policy which can be viewed at – Understanding the national data opt-out - NHS Digital

Choosing your vaccination invitation preference

We have set up a service for people to choose whether they receive invitations and reminders to attend for COVID-19 vaccinations and further information can be found at – www.nhs.uk/covid-invite-preferences.

When you access this service, we need to verify your identity. You will need to provide your name, date of birth, and either your NHS Number or postcode. There is a facility to find an NHS number if you do not know it at – Find your NHS number - NHS (www.nhs.uk).

You will also need to have an email address or mobile phone number that you have registered with your GP, and is available in the – Personal Demographics Service.

Once you have made your preference, your choice is saved against your NHS number. This is the minimum amount of information that we need to provide this service.

We also record and store audit data each time you use the service, including the date and time and internet protocol (IP) address. This is stored to help us monitor the service and protect the service from malicious use. This data is stored on secure servers in the European Economic Area.

Whilst you will no longer receive COVID-19 vaccine invites for that particular campaign, your details will continue to be processed for the purposes of managing and monitoring the progress of the COVID-19 programme.

If circumstances were to change, for example should the impact of COVID-19 significantly worsen, we may consider whether we have compelling grounds to send vaccination invitations irrespective of any preference set.

Setting your COVID-19 contact preference using this central service will not stop other organisations such as your GP practice from sending you invitations for vaccinations.

NHS Genomic Medicine Service: Whole Genome Sequencing

How we use personal data to provide genomic testing

NHS Genomic Medicine Service

Purposes and controllers

NHS England is commissioning an NHS Genomic Medicine Service. This service is available to clinicians anywhere in England and it gives them a facility to order tests based on the analysis of their patients' whole genome – their genetic makeup.

The service is provided by seven Genomic Lab Hubs each of which is made up of number of NHS Trusts or NHS Foundation Trusts ("GMS NHS Trusts") which provide testing, interpretation and reporting services.

The GMS NHS Trusts together with NHS England are responsible as joint controllers under data protection legislation for the processing of personal data to provide the NHS Genomic Medicine Service. A list of the GMS NHS Trusts with links to their online privacy notices is presented below.

The labs use a computer system called the National Genomic Information System (NGIS), which NHS England has commissioned for them from Genomics England Ltd. Genomics England is a processor for the provision of the NGIS, acting on the instructions of NHS England for the Trusts that provide lab services.

How personal data is used for your genomic test

The human genome is made up of 3 billion letters of DNA (A, T, C and G). Whole genome sequencing is a technique that is used to ‘read’ these letters and finds their order one by one. The digital record of this sequence can be then analysed by computers to produce information to inform the diagnosis and treatment of rare conditions or cancer.

When a clinician orders a whole genome sequence test using the new service, he or she will send a blood or tissue sample with an order form to a pathology laboratory that has been designated to perform the type of test being requested in the local area. This lab will extract the DNA from the sample and send it to a specialist lab that puts the DNA into a tube or “well” in a rack or “plate” of other samples. In this way the samples are organised so that they are matched to the right patient when they are analysed, ensuring that the patient gets the result that relates to their test. As a double check the lab that extracted the DNA keeps a DNA signature from the sample, which is then compared to the sequenced DNA.

The plates of samples are sent to a company called Illumina that carries out the whole genome sequencing process. Illumina is contracted to Genomics England to provide this service.

A digital file is created with the unique 3 billion letters, and this is sent to Genomics England’s Bioinformatic Pipeline. This system analyses the DNA sequence, guided by the type of test that has been ordered, and creates an automatic interpretation of parts of the genome that are relevant to the patient’s condition. The facts that are presented in this automatic interpretation are further interpreted by clinical scientists in the Genomic Lab Hubs.

The NGIS is accessed by lab staff who have access permissions enabled that are appropriate to their role. As this is a national service, lab staff with access enabled can see the genomic records of any patient that has had a test requested for them. This enables clinical scientists that specialise in a particular condition to provide interpretation services for patients outside their area.

Genomics Multi-Disciplinary Teams

The GMS NHS Trusts host meetings of multi-disciplinary teams (MDTs) which review individual cases. Clinicians from the GMS Trusts and referring clinicians attend these meetings to collaborate in reviewing their cases.

The MDT meetings are supported a Genomics Management System that allows the display and annotation of genomic information from the National Genomic Information System. The system is accessed only by authorised individuals in NHS Trusts.

Managing and improving the service

Personal data is processed for the following purposes by the GMS NHS Trusts and NHS England.

- The improvement of delivery of direct care (clinical care), which includes supporting the development of knowledge of genomic variants as well as maintaining and improving the quality of the service;
- The improvement of the service, driving improvements in access, effectiveness and efficiency.

Data that identifies patients directly is not disclosed outside the team providing care for these purposes. The data is de-identified or aggregate numbers.

NHS England receives a monthly Patient Level Contract Monitoring Dataset from each of the GMS NHS Trusts for its commissioning purposes. This is collected by NHS Digital and provided to NHS England in de-identified form – see Data Services for Commissioners.

Research

Every patient that is offered a whole genome test is asked if they want to donate your sample (blood / saliva / tissue, etc.), genome sequence and health data for research co-ordinated by Genomics England.

For patients who agree, NHS England, on behalf of the Trusts that provided that provided the genomic test will allow Genomics England to access personal data held in the NGIS for inclusion in the National Genomic Research Library. This is a secure national database of genomic and health data managed by Genomics England.

Genomics England Ltd is controller under data protection legislation for the purposes of the National Genomic Research Library.

Categories of personal data

The following types of personal data are processed:

- Patient Identifiers including NHS Number
- Demographics – name, address, date of birth, ethnicity, registered GP
- Clinical pathway
- Family identifiers – where relevant

- Clinical Indicators – nature of condition, details of condition
- Clinical measurements and observations relevant to condition specific to cancer or rare and heritable disease pathways
- Clinical ethnicity and clinical sex details
- Details of genomic testing and related procedures – e.g. the type of test performed
- Link to previous requests and tests
- Whole Genome Sequence
- Special Categories of Personal Data include
    - Racial or ethnic origin
    - Genetic data
    - Health data

Joint Controller Agreement

NHS England and the GMS NHS Trusts have entered into a Joint Controller Agreement which provides a framework for how they will work together to ensure that they comply with data protection requirements when they process personal data for the purposes of the Genomic Medicine Service. In this agreement they make the following commitments

- They will make sure that they are transparent about their joint purposes for Processing Personal Data
- They will make sure that anyone who wants access to their Personal Data, or to exercise other rights under Data Protection Law, have an easily accessible point of contact to make their request (see the GMS NHS Trusts privacy notices below)
- They will make sure that their data protection policies and procedures properly govern their processing of personal data
- They will make sure that personal data that they process, or is processed on their behalf by processors, is protected by appropriate technical and organisational security measures
- They will make sure that their personnel have a confident understanding of their data protection responsibilities
- They will not transfer personal data outside the European Economic Area unless appropriate legal safeguards are in place in accordance with data protection law.

The GMS NHS Trusts and privacy notices

North West Genomic Laboratory Hub

- Manchester University NHS Foundation Trust
- The Christie NHS Foundation Trust
- Liverpool Women's NHS Foundation Trust

North East and Yorkshire Genomic Laboratory Hub

- The Newcastle Upon Tyne Hospitals NHS Foundation Trust
- The Leeds Teaching Hospitals NHS Trust
- Sheffield Children's NHS Foundation Trust

South West Genomic Laboratory Hub

- North Bristol NHS Trust
- Royal Devon and Exeter NHS Foundation Trust

Central and South Genomic Laboratory Hub

- Birmingham Women's and Children's NHS Foundation Trust
- University Hospitals Birmingham NHS Foundation Trust
- Oxford University Hospitals NHS Foundation Trust
- Salisbury NHS Foundation Trust
- University Hospital Southampton NHS Foundation Trust

East Genomic Laboratory Hub

- Cambridge University Hospitals NHS Foundation Trust
- Nottingham University Hospitals NHS Foundation Trust
- University Hospitals of Leicester NHS Trust

London North Genomic Laboratory Hub

- Great Ormond Street Hospital for Children NHS Foundation Trust
- The Royal Marsden NHS Foundation TrustThe Royal Marsden NHS Foundation Trust
- Imperial College Healthcare NHS Trust
- Barts Health NHS Trust
- University College London Hospitals NHS Foundation Trust
- Royal National Orthopaedic Hospital NHS Trust
- Royal Free London NHS Foundation Trust

South East Genomic Laboratory Hub

- Guy's and St Thomas' NHS Foundation Trust
- King's College Hospital NHS Foundation Trust
- St George's University Hospitals NHS Foundation Trust
- Royal Brompton and Harefield NHS Foundation Trust

Legal basis for processing

For GDPR purposes NHS England's and the GMS NHS Trusts' lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'

For the processing of special categories (health) data the bases are

9(2)(h) – '…health or social care…' – for the provision of the testing service

9(2)(g) – '…necessary for reasons of substantial public interest…' Underpinned by paragraph 8 (Equality of opportunity or treatment) of Schedule 1 to the Data Protection Act 2018 – for processing of racial or ethnic origin

9(2)(j) – '…research purposes…' – for dissemination to Genomics England Ltd. for inclusion in the National Genomic Research Library

Data Analytics

How we use de-identified personal data to support our Purpose: "To lead the NHS in England to deliver high-quality services for all"

Data Analytics and NHS England's Purpose

Supporting NHS England's Purpose

NHS England needs information to achieve its Purpose – *To lead the NHS in England to deliver high-quality services for all*. Our analysis of de-identified personal data relating to peoples' NHS care is essential to providing us with much of this information.

Our purpose statement provides clarity on what NHS England is seeking to achieve. It drives both 'what' we do (how we add value and what our priorities are) as well as 'how' we operate (our values, behaviours and accountabilities, and structures). NHS England's operating framework sets out what we will do to achieve our Purpose and how we will do it:

- enabling local systems and providers to improve the health of their people and patients and reduce health inequalities;
- making the NHS a great place to work, where our people can make a difference and achieve their potential;
- working collaboratively to ensure our healthcare workforce has the right knowledge, skills, values and behaviours to deliver accessible, compassionate care;
- optimising the use of digital technology, research and innovation; and
- delivering value for money.

Activities to deliver these, and all of our public tasks are underpinned by functions and duties set out in legislation. Our statutory functions relate to, for example, the commissioning of primary care services, some secondary care services, and to the administration of screening services. A selection of our statutory duties from the NHS Act 2006 is set out below:

13C. Duty to promote NHS Constitution

13D. Duty as to effectiveness, efficiency etc.

13E. Duty as to improvement in quality of services

13F. Duty as to promoting autonomy

13G. Duty as to reducing inequalities

13H. Duty to promote involvement of each patient

13I. Duty as to patient choice

13J. Duty to obtain appropriate advice

13K. Duty to promote innovation

13L. Duty in respect of research

13M. Duty as to promoting education and training

13N. Duty as to promoting integration

13NA. Duty to have regard to wider effect of decisions

13NB. Guidance about discharge of duty

13NC. Duties as to climate change etc

13ND. Guidance about discharge of duty under section 13NC etc

13O. Duty to have regard to impact on services in certain areas

13P. Duty as respects variation in provision of health services

As a statutory organisation NHS England is legally obliged to perform its functions and duties. We cannot perform them without a clear understanding of how the NHS is performing in relation to them. It essential that we have information about all aspects of NHS services and its operating environment to achieve our Purpose.

Much of the information that we need can only be produced by analysing data obtained from providers of NHS care. The data that we analyse is de-identified or 'pseudonymised' personal data. This is data that relates to individuals, with for example information about the care they have received, but with no data items that identify them directly. NHS England may analyse this data to facilitate any of its statutory functions and duties. As the data is de-identified people's confidentiality is respected.

Analytical environments

The Unified Data Access Layer (UDAL) is our main analytical environment. It is a secure de-identified environment, technically and organisationally segregated both from source environments holding identifiable data and from the environment in which pseudonymisation is performed. (Our legacy environments use the same processes).

The general principle in UDAL is that users only have access to the data for which they require access. No data outside of "public" data is available to all users as standard. This public data includes published data as well as some additional internally derived reference data. It does not include any patient level data.

Access to UDAL for new users must be approved by line managers, and the Data Operations team being led by the Information Asset Owner. Further approval and justification is required for access to the restricted pseudonymised datasets.

Data collections

NHS England has a power to collect and analyse information from health organisations, when directed to do so by the Secretary of State for Health and Social Care, using powers under the Health and Social Care Act 2012. When acting under directions, NHS England

may collect and analyse personal data, including confidential information for purposes set out in the direction. When directed NHS England has a power to require the provision of data by health providers.

When pseudonymised and transferred to our de-identified environments the data may be analysed for purposes relating to any of our statutory functions or duties as described above, provided that this is not incompatible with the purpose for which the data was collected.

Merger with NHS Digital

In February 2023 NHS Digital merged with NHS England. NHS England acquired many of NHS Digital's statutory powers and duties and has also become controller responsible for processing previously conducted by NHS Digital.

Before the merger, both NHS England and the Secretary of State for Health and Social Care could give a direction requiring NHS Digital to collect and analyse data from providers of NHS services.

When directed, NHS Digital could then require the provision of the data by these providers. This data could include fully identifiable personal data and confidential information. NHS Digital would then disseminate the data in pseudonymised form to NHS England for our analysis. The data processed by NHS England analysts was considered 'anonymous in context'.

With the merger, the Secretary of State can make similar directions to NHS England, and all existing directions to NHS Digital are to be read as if given by the Secretary of State to NHS England. The consequence of this is that NHS England can collect and analyse fully identifiable personal data when directed to do so.

As NHS England is now responsible for the de-identification process, we now have the technical ability within the organisation to re-identify the data held in pseudonymised form. So, it can no longer be considered 'anonymous in context'. To prevent re-identification and maintain confidentiality, NHS England must separate the processing of identifiable data collected under directions from the derived pseudonymised data held in our analytical environments.

To this end the Secretary of State has given the NHS England De-Identified Data Analytics and Publication Directions 2023. These require NHS England to put in place arrangements for the governance of ongoing processing of de-identified data that it previously obtained from NHS Digital and a framework for the future analysis, linkage and de-identification of

data NHS England needs to access in the exercise of its functions in connection with the provision of health services.

As the directions mandate the processing by NHS England of de-identified personal data in support of its functions, the lawfulness of processing such data for ***any*** purpose that is "…not incompatible with the purpose for which the identifying data was obtained…" is explicit and transparent. This depends on the segregation of pseudonymised and identifiable environments as explained above.

The links below give access to directions given to NHS Digital by NHS England and the Secretary of State.

- NHS England Directions
- Secretary of State Directions

See also: Data Services for Commissioners

Sources of the data

The information may be collected by NHS England under directions, from any organisation that provides health services to the NHS, including NHS Trusts, NHS Foundation Trusts, GP Practices and other primary care providers and local authorities.

Categories of personal data

The details of the individual collections are specified in the directions. This may include records representing individual items of care, or summarised information including just numbers.

Where information about individual patients and their care is collected, this will usually include their NHS Number, other similar identifiers, postcode and date of birth. These are needed to make sure that the data is correct, and to allow linkage to other data. The data will include information about the health care received, administrative information, and may include ethnicity.

As described above identifiable personal data collected under directions is pseudonymised and transferred to our de-identified environments for analysis.

Categories of recipients

Within NHS England personal data collected under directions is processed by teams authorised to manipulate the data in identifiable form, to prepare it for the purpose set out in the direction. This processing may involve linkage to other datasets held by NHS England.

Data is released in pseudonymised form to NHS England's de-identified environments, in accordance with the Analytics Directions described above. From here it may be accessed by analysts.

Data may be released in identifiable form only where there is an established legal basis, for example approval by the Secretary of State under the Health Service (Control of Patient Information) Regulations 2002 ('section 251 support') – see for example Assuring Transformation.

Data may be released to other organisations in a form that is anonymised in line with the Information Commissioner's Anonymisation code of practice, or in identifiable form where there is an established legal basis. All requests for data from other organisations are dealt with by the Data Access Request Service.

Legal basis for processing

For UK GDPR purposes NHS England's lawful bases for processing are:

Article 6(1)(c) – '…legal obligation…' when acting under directions from the Secretary of State, and

Article 6(1)(e) – '…exercise of official authority…' when processing in support of our statutory functions.

For the processing of special categories (health) data the conditions may be one or more of articles

9(2)(h) – '…health or social care…';

9(2)(i) – '…public health…'

9(2)(j) – '…research purposes or statistical purposes…'.

How we use your information

How we use personal data to perform our functions.

Coronavirus (COVID-19) Response

How we use personal data to support the NHS response to the COVID-19 pandemic.

NHS COVID-19 Data Store

Purposes for processing

NHS England is providing a national response to the COVID-19 pandemic. Data is providing us with evidence to help keep the public safe and provide the best possible response to the virus. We are working with multiple companies under strict contractual controls to support our approach.

To support this, we have established an NHS COVID-19 Data Store. This will ensure that data can be used by the NHS and government to look at trends

to monitor the spread of the virus and implement appropriate measures to ensure services and support is available to patients. For example, the data can be used to look at bed capacity in hospitals or the number of ventilators available in a particular area.

What data is included?

The data required to support the response to COVID-19 is obtained from a number of sources. The datasets are listed in the COVID-19 Datastore Reference Library.

We are working with our partners to ensure that the data in the store is comprehensive. Both NHS Digital and The UK Health Security Agency (UKHSA) are providing data to the store. The datasets provided by NHS Digital are pseudonymised prior to going into the NHS Data Store to ensure that individual patients are not identifiable.

The following datasets are received in identifiable form directly from UKHSA and the Intensive Care National Audit and Research Centre:

- NHS England receives identifiable data from UKHSA. This includes Lab test data
- Data from the COVID-19 Hospitalisation in England Surveillance System (CHESS) database.
- Intensive Care National Audit and Research Centre (ICNARC) – Care provided to COVID-19 patients and discharge data

This data is validated by NHS England and pseudonymised before it is uploaded to the NHS COVID-19 Data Store. All data processed in the NHS COVID-19 Data Store is either pseudonymised, anonymised or aggregated and therefore does not identify any individual.

Categories of personal data

The NHS COVID-19 Data Store holds personal data representing aspects of individual patient's access to health services including diagnosis, treatment and patient management

information. The personal data held in the NHS COVID-19 Data Store is pseudonymised in line with Information Commissioner's Office (ICO) guidance and best practice and does not identify individual patients.

Organisations and their roles

NHS England and the Department for Health and Social Care are the legal organisations working together to ensure data can be collected and processed safely and securely. NHS England is the Data Controller for the data held in the data store and there is an agreement in place which sets out the roles and responsibilities of each organisation when we are working jointly.

Other organisations which are supporting the work on the NHS COVID-19 Data Store either have a commercial contract (which covers supporting the technology element of the store); a data processing contract; or an honorary contract where direct access to data is required to support NHS requirements.

The NHS COVID-19 Data Store sits on a Microsoft Azure platform under contract with NHS England. Within that secure cloud processing environment, Palantir (acting under instruction from NHS England) manage their platform which is called Foundry.

Palantir, have built analytical dashboards for access by NHS England staff, together with staff in the following organisations working under contract: Faculty AI, McKinsey and Deloittes. Data which is pseudonymised, is only available to staff working under contract with NHS England or DHSC.

The table below sets out each organisation and their role and contract types with level of access to data:

Organisation	Role	Contract Type	Level of Access
Faculty Ltd	Support and help improve the NHSX Innovative Data Analytics	G-Cloud Call off Contract with DHSC and Honorary contracts with NHS England	Pseudonymised/Aggregate/Anonymous

	capacity and capability		
McKinsey	Support and help improve the Innovative Data Analytics capacity and capability	Contract with DHSC and Honorary contracts with NHS England	Pseudonymised/Aggregate/Anonymous
Deloittes	Support and help improve the Innovative Data Analytics capacity and capability	Contract with DHSC and Honorary contracts with NHS England	Pseudonymised/Aggregate/Anonymous
ANS Group	Support and platform build only	Contract with NHS England through SBS cloud solution framework	Pseudonymised/Aggregate/Anonymous
Palantir/using their Foundry platform	Set up platform for NHS COVID 19 Data Store	G-Cloud Call off data processing contract with NHS England	Pseudonymised/Aggregate/Anonymous

Who will access the data?

The secure NHS COVID-19 Data Store brings together and protects accurate, real-time information to inform strategic and operational decisions in response to the current pandemic in one place. A number of different dashboards will be used by different organisations to support the response as shown below:

- a public Information Dashboard, showing statistics on cases of coronavirus and deaths associated with coronavirus in the UK, updated daily
- a Strategic Decision Makers Dashboard, providing a national summary of situation report (SitRep) information, alongside modelling, simulations and analysis. These dashboards are designed to help senior national and regional officials to make policy and strategic decisions in response to Covid-19. Only Government and senior regional analysts and managers are given access to this dashboard.
- an NHS Operational Dashboard, providing local NHS and local government organisations with a clear picture of what is happening both across the country and specifically in their area so that they can take the right local action.

Legal basis for processing

For GDPR purposes NHS England's basis for lawful processing is

Article 6(1)(c) – '…compliance with a legal obligation…'.

Article 6(1)(e) – '…exercise of official authority…'.

For special categories (health) data the bases are

Article 9(2)(h) – '…health or social care…';

Article 9(2)(i) – '…public health…';

Article 9(2)(j) – '…archiving…research…or statistical purposes…'.

Our mandate to process confidential patient information, setting aside the duty of confidence, has been a notice from the Secretary of State for Health and Social Care under regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002 ("COPI notice"). This supplements our permissive powers under regulation 3(3) to process confidential patient information for purposes related to communicable disease and other risks to public health.

A similar notice to organisations providing health services, GP practices, Local Authorities and Arm's Length Bodies of DHSC provided the basis for requiring the dissemination of

confidential patient information to NHS England and NHS Improvement for Covid-19 Purposes.

These notices expired on 30h June 2022.

From 1 July 2022 NHS England will continue to receive and process the confidential patient information that is necessary for Covid-19 Purposes. Although no longer mandated, the dissemination of confidential patient information to NHS England by organisations that were previously required to do so by the their COPI notice remains lawful as they can apply their powers under regulation 3(3).

OpenSAFELY – the Coronavirus (COVID-19) Research Platform

Teams Under Pressure

Purposes for processing

The purpose of *"Teams Under Pressure"* is to offer NHS line managers the means to effectively support and lead their teams during and after Covid19. This offer includes providing a web-based portal through which NHS managers can apply for coaching and mentoring along with online resources and toolkits.

Sources of data

Participation for this service is voluntary, and personal data is collected via a dedicated NHS England website. Contact data will be used to facilitate training and will be shared with training providers. It is not mandatory for participants to provide any diversity information. But those who do submit this data, be assured that it will only be used for equality monitoring and will not be shared outside NHS England.

Categories of personal data and recipients

The data voluntarily provided will be: name, email, contact number to be used to support the scheduling of sessions, issuing invitations and sending reminders. Additionally, other data voluntarily provided will be: NHS organisation, region, role, gender, marital status, ethnicity, religious belief, disability, age and sexual orientation. This Special Category data will only be used for diversity monitoring and evaluation and will not be shared with anyone else. The evaluation will be carried out by NHS England.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is: *Article 6(1)(e) – '…exercise of official authority…'* and for processing special categories (health) data the basis is: *Article 9(2)(h) – '…health or social care…'.*

National COVID-19 Chest Imaging Database (NCCID)

The NCCID privacy notice can be found on the NHSX website.

COVID-19 Public Inquiry: Privacy Notice for NHS England Staff

The UK COVID-19 Inquiry (the Inquiry) has been set up to examine the UK's response to and impact of the COVID-19 pandemic. NHS England played a vital role in responding to the pandemic and will need to respond to questions and requests received from the Inquiry.

Our activity relating to the Inquiry will broadly fall into two categories:

- Preparation: We need to prepare for the questions and requests which the Inquiry may potentially ask us.
- Response: We will need to respond to the questions and requests which we receive from the Inquiry.

The below information only relates to NHS England's use of personal data for purposes relating to the Inquiry.

Further information about the terms of reference and scope of activity of the Inquiry can be found here: covid19.public-inquiry.uk

Purposes for processing

In responding to the Inquiry, NHS England will:

- help support colleagues and former colleagues
- ensure information (including personal data) is collected, shared and used in line with our internal policies and legal requirements
- manage our relationship with the Inquiry
- ensure we submit high quality evidence and
- respond to findings and lessons identified

The purposes for using and sharing your data will be:

Preparing for the Inquiry: As the scope and terms of reference scope of the Inquiry are publicly available, and as NHS England's role in responding to the pandemic are known, NHS England are able to prepare for the questions which the Inquiry may ask us in advance.

Such preparatory work may include accessing and reviewing personal data relating to our colleagues in relation to their role in responding to the pandemic.

Responding to the Inquiry: When NHS England receive questions from the Inquiry, it is likely that NHS England will need to access and review the personal data of its colleagues in relation to their role in responding to the pandemic. NHS England may also need to share personal data relating to colleagues and former colleagues with the Inquiry where necessary to answer questions raised by the Inquiry. NHS England will typically only share personal data relating to senior NHS England colleagues with the Inquiry unless the sharing of junior colleagues' personal data is essential to answer a question.

Categories of personal data

The information we will process for these purposes includes:

- Information which identifies you (e.g. your name);
- Your work-related contact information (e.g. your work email address);
- Your current contact information (e.g. if you no longer work for NHS England – this could include your home address, personal phone number);
- Information about your role with NHS England (e.g. Your job title, contract start date and end date);
- Personal information contained in communications and official documents (e.g. your name, communications you may have sent or received)

Sources of the data

For the purpose of the Inquiry, we will mainly use personal data from the following sources:

Information NHS England already holds: NHS England will review and share communications and documents created for the purpose of responding to the COIVD-19 pandemic which may contain your personal data relating to your role with NHS England.

Information which you provide for the purpose of the Inquiry: You may provide NHS England with further personal information if NHS England engage with you in relation to the Inquiry

Categories of recipients

NHS England will disclose personal data to the Inquiry and where NHS England is instructing other parties, such as external lawyers, to support its Inquiry related activities.

NHS England may share your personal data with such parties and these organisations only where it is required to complete the tasks assigned to them by NHS England.

Retention period

Your data is already being processed in line with NHS England's existing retention policies. More information is available here: NHS England » NHS England as a data controller

For personal data that is disclosed to, and subsequently processed by the Inquiry, please see the Inquiry website for more details: covid19.public-inquiry.uk

Legal basis for processing

Under the UK General Data Protection Regulation (UK GDPR) NHS England's legal basis to use your information for purposes related to the Inquiry are:

- Public task: As a public authority, NHS England can use your information to perform its public tasks where that use is in the public interest. Those tasks extend to the activities NHS England need to perform to prepare and respond to the requests NHS England receive from the Inquiry (Article 6(1)(e) of UK GDPR).
- Legal obligation: NHS England can use your personal data to meet its legal obligations. Under the Inquiries Act 2005, the Inquiry may require NHS England to provide evidence, which may include your personal data, which relates to a matter in question at the inquiry. (Article 6(1)(c) of UK GDPR).

NHS England also need an additional legal basis in the UK GDPR and the Data Protection Act 2018 (DPA 2018) to use data which is particularly sensitive such as information about a person's health, ethnicity, religion, trade union membership. These types of data are called 'special category data'.

NHS England will not typically be required to use or share your sensitive information for the purposes of the Inquiry but it could potentially be relevant, depending on the specific questions NHS England receive from the Inquiry. For example, NHS England may be required to confirm that a senior member of staff was unable to make a decision because they were not working at the relevant time due to illness.

If it is necessary to use or share your sensitive information for the purpose of the Inquiry, NHS England will rely on the following additional legal basis:

- Substantial public interest: NHS England's use of your information is necessary for reasons of substantial public interest based on UK law which is proportionate to the purposes (set out above). (Article 9(2)(g) of UK GDPR). NHS England have a statutory obligation under the Inquiries Act 2005 to fulfil the purpose and that statutory obligation is NHS England's condition for relying on substantial public interest as its legal basis (the condition is set out in paragraph 6 of Schedule 1 to the Data Protection Act 2018).
- Legal advice: NHS England may use your sensitive personal data for the purpose of obtaining legal advice. (Article 9(2)(f) of UK GDPR). NHS England can rely on this legal basis when it is necessary to share your personal data with its legal advisors for the purposes of preparing for and responding to the Inquiry.

Our Services

How we use personal data to commission health services and for our functions in connection with the provision of NHS services.

Providing Online Consultation Services

Purposes for processing

NHS England have supported the wider NHS by commissioning online consultation services for GPs and NHS Trusts. For the purposes of GDPR:

- NHS England is a joint controller with GPs for the provision of the eConsult online consultation service
- NHS England is a joint controller with NHS Trusts for the provision of the Attend Anywhere online consultation service

Sources of the data

For all platforms: Personal data required to support the provision of online consultations is collected directly from patients as part of registering for or engaging with the platforms.

For eConsult only: Where patients utilise eConsult via the NHS App, the data they supply will be matched with data held by the NHS Login service in order to verify their identity.

For Attend Anywhere only: Additional personal data about colleagues are collected from staff in GPs, NHS Trusts for the purposes of user account creation and management.

Categories of personal data

For eConsult: Patients registered with GP's using the platform

For Attend Anywhere: Patients referred to NHS Trusts using the platform, staff of NHS Trusts using the platform and staff of NHS England

Categories of recipients

For eConsult: GPs only

For Attend Anywhere: NHS Trusts (identifiable patient data), NHS England (clinician data and de-identified consultation metrics), Advanced Solutions (clinician data and de-identified consultation metrics to provide a technical service desk) and Edge (clinician data and de-identified consultation metrics to provide a service evaluation).

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing data associated with GPs' online consultation services is Article 6(1)(e) '…exercise of official authority…'. NHS England does not receive or process any special categories of personal data for this purpose.

For GDPR purposes NHS England's lawful basis for processing data associated with NHS Trusts' online consultation services is Article 6(1)(e) '…exercise of official authority…'. NHS England does not receive or process any special categories of personal data for this purpose.

Patients registered with GP Practices

Purposes for processing

NHS England has a legal duty under Schedule 3, Part 2, paragraph 17 of the National Health Service (General Medical Services Contracts) Regulations 2015 to keep and maintain a list of all patients registered with GP Practices in England. This list is held in the National Health Application and Infrastructure Services (NHAIS) and Primary Care Registration Management (PCRM) systems. These systems also hold data about patients registered with GP practices in Wales and the Isle of Man.

The data are used to provide Primary Care Support Services. NHS England has a contract with Capita Business Services Ltd, operating as Primary Care Support England (PCSE) to provide these services as NHS England's data processor which includes:

- Moving paper patient records between practices and into storage when patients leave or move practices
- Storing paper records of unregistered and deceased patients
- Sending letters to patient to inform them of their NHS number when one is first allocated
- Providing the cervical cytology call and recall administrative service
- Delivering prior notification lists of patients eligible for screening to GPs
- Making payments to NHS Ophthalmic practitioners for NHS services provided
- Making payments to GP practices based on lists of registered patients, and specific payments for childhood vaccinations and immunisations
- Notifying GP practices when mail has been returned from a patient's registered address (by setting an 'FP69 flag') so that GP practices can contact the patient to establish if they have moved. If no response is received from the patient or GP practice within 6 months, the patient is removed from the practice's list.

- Writing to patients on behalf of Primary Care commissioners with regards to provision of primary care services or assignment to a GP Practice list.

- Processing new patient registrations and de-registrations at GP practices to maintain accurate lists of numbers of patients at GP practices. Where we reasonably believe a patient has moved home address and this is outside of their GP practice's catchment area, we contact the patient (by letter, email or SMS using the NHS Notify service)to confirm their home address and inform them that if they do not respond within 30 days, we will begin the process of removing them from their GP practice's patient list.

- Writing to patients to inform them when they have been removed from their GP Practice list
- Conducting audits and reconciliations of GP Practice lists to ensure list sizes are accurate.

The data from the NHAIS and PCRM is used to update the Personal Demographics Service (PDS). This provides information for hospitals, screening programmes, Child Health systems and other health providers making sure that they know their patients' current GP practice and can access other essential information such as the National Care Records Service (formerly the Summary Care Record).

NHS England Regional Local Teams (RLTs) and Clinical Commissioning Groups (CCGs) (where delegated) may also undertake necessary processing of a limited subset of these data (e.g. patient name, address, postcode and NHS number) for example when managing practice closures and list dispersals (the process used to allocate patients to neighbouring GP Practices). This processing is necessary to inform patients of their reregistration options and 'Choice' as required under the NHS Constitution.

Sources of the data

The data are transferred automatically from GP practice systems into the NHAIS and PCRM systems. The data is also updated by Primary Care Support England after notifications from data subjects themselves.

Categories of personal data

The categories of personal data held on the systems are:

- Name – including any previous names, unless name changes are the result of adoption, gender reassignment or witness protection schemes
- Current and historic addresses and whether the address is a registered nursing home
- Dates of Birth

- Gender
- Place of Birth
- NHS number
- Cervical Screening history
- Special allocation scheme status
- Current and Previous GP practice details
- GPs Banking details

Categories of recipients

Statistical information (numbers) produced from NHAIS systems is shared with other organisations to enable them to fulfil their statutory obligations, for example the Office of National Statistics, UK Health Security Agency and local authorities for their public health purposes. Personal data may also be shared with the approval of NHS England's Caldicott Guardian when he is assured that confidentiality is respected, for example when hospitals need to update their records for direct care purposes or to support specific research projects with ethical and or Health Research Authority approval.

Legal basis for processing

For UK GDPR purposes NHS England's basis for lawful processing is Article 6(1)(e) – '…exercise of official authority…'. For special categories (health) data the basis is Article 9(2)(h) – '…health or social care…'

Primary Care Commissioning

Purposes for processing

NHS England is responsible for commissioning high quality primary care services for the population of England. NHS England's commissioning policy is to move towards more place based, clinically led commissioning and is sharing or delegating commissioning of primary medical care services to Clinical Commissioning Groups (CCGs). NHS England retains responsibility for payment of GPs, Dentists and Opticians. NHS England and delegated CCGS also have responsibility for the assignment of unregistered patients to GP practices, and for the management of list transfers when practices close.

General Practice

GP Payments

NHS England is responsible for paying GP Practices for their services. GP practices are paid on the basis of the number of patients on their list. This is obtained from the registered

patient list held by NHS Digital on behalf of NHS England. In addition to this GPs are paid for their performance under the Quality and Outcomes Framework (QOF). NHS Digital collects information under directions from NHS England about General Practice (GP) achievement under QOF. This information is used to calculate GP payments for the current financial year, and to set aspiration payments for the following year. NHS Digital run other QOF reporting collections throughout the year, not related to payment. The QOF data is extracted by NHS Digital from GP Practice systems. The data extracted is in the form of numbers for the QOF indicators and does not include personal data.

Disclosures of personal data to NHS England

NHS England may require access to personal data held by GP practices in circumstances described in the *Confidentiality and Disclosure of Information: GMS, PMS and APMS Code of Practice*. This is established under directions from the Secretary of State for Health. These circumstances are:

- Where NHS England is investigating and assuring the quality and provision of clinical care, for example in relation to a complaint.
- Where it is needed in relation to the management of the contract, for example where remedial action, or termination of the contract/agreement is being considered (e.g. because of poor record keeping)
- Where NHS England considers there is a serious risk to patient health or safety
- Investigation of potential fraud or any other potential criminal activity

Patient assignments and list transfers

The process from managing patient assignments is described in the Primary Medical Care Policy and Guidance Manual. NHS England or a CCG will receive the names, addresses and other personal details (not health information) of unregistered patients who have requested registration at a GP Practice. NHS England or a delegated CCG will receive the personal details of patients registered at a GP practice that has closed or is due to close in order to offer alternative registration.

Unregistered patients

NHS England is responsible for the manual records of patients who are not currently registered with a GP Practice, and the deceased. These records are held by Primary Care Support England on our behalf.

GP contracts

GP contracts are held in NHS England's local offices. The contract includes the name of the contract holder(s).

Community Pharmacy

NHS England is responsible for putting arrangements in place so that drugs and appliances ordered on NHS prescriptions can be supplied to patients. These are known as 'Pharmaceutical Services' and are provided by pharmacy contractors (such as retail pharmacy outlets), dispensing appliance contractors, and dispensing doctors (collectively referred to as 'contractors' in this section of this privacy notice).

Pharmaceutical lists

In order to provide Pharmaceutical Services, pharmacy and dispensing appliance contractors must first be included in a list for their local area, called a pharmaceutical list, which is managed by NHS England. The management of pharmaceutical lists by NHS England is laid down in the National Health Service (Pharmaceutical and Local Pharmaceutical Services) Regulations 2013.

NHS England will receive personal data and process it as is necessary for the purposes of managing pharmaceutical lists in accordance with the Regulations. In particular, such personal data may:

- include details about contractors (including directors of a company or partners of a partnership), contractors' staff, referees, applicants wishing to join the pharmaceutical list, and third parties making submissions on an application;
- be obtained from the individual to whom it relates (for example, an individual pharmacist applying to join a pharmaceutical list) or from a third party (for example, a company wishing to be included in a pharmaceutical list which provides details about its directors and superintendent pharmacist);
- be shared with third parties where appropriate (e.g. notification of decisions as required by the Regulations).

Certain individuals involved in providing Community Pharmacy services must submit information about their fitness to practise to NHS England, which may include special categories of personal data and data relating to criminal convictions and offences. This information may also be obtained from or shared with other organisations, such as the General Pharmaceutical Council (GPhC), in accordance with the Regulations. NHS England will use this information to consider whether a person is fit to practise and take action where there are concerns.
NHS England has a contract with Primary Care Support England (PCSE) to administer applications in relation to the pharmaceutical lists on behalf of NHS England.

Dispensing doctors

Dispensing doctors (GPs who may dispense drugs and appliances directly to patients where certain conditions are met) are included in a separate list managed by NHS England.

Patients may make an application to NHS England to request that their GP provide them with dispensing services. These applications contain the personal data of patients and may also include special categories of personal data. NHS England may obtain and process such personal data for the purposes of determining the application.

Local Pharmaceutical Services

Some contractors are locally commissioned to provide Local Pharmaceutical Services (LPS) and are included in separate lists managed by NHS England. NHS England may obtain and process personal data for the purposes of managing LPS contractors in a similar manner to that outlined above.

Payment for Community Pharmacy services

Contractors are paid for the number of prescriptions that they dispense. Each month they send their prescriptions to the NHS Business Services Authority (NHS BSA) who acts on behalf of the Department of Health and Social Care. These are sent either electronically or by courier for paper documents. A small number of prescriptions are shared with NHS England and other relevant organisations where this is necessary for the purposes of investigating possible prescription errors or fraud. These prescriptions contain the personal data of patients, including special categories of personal data.

Medicines Usage Reviews

This is a service usually provided in a pharmacy to help a patient use their medication more effectively. However, in some cases a pharmacy will need to seek permission from NHS England to provide this service by telephone or in a patient's own home. This will require the pharmacy to share the patient's name and address with NHS England.

Dentists

Payment of dentists

Dentists are paid by the NHS Business Services Authority (NHS BSA) acting for the Department of Health and Social Care. NHS England receives service activity figures, which do not include personal data, from NHS BSA for reconciliation and adjustment for under-payments.

Appeals

A patient may appeal to NHS England about any aspect of their dental care. For example, if a patient is assessed that he or she doesn't meet criteria for a NHS funded specialist service. The appeal information includes personal details and specific details of clinical condition.

Contracts

Commissioning contracts for dentists are held in NHS England's local offices, and these may identify the individual responsible for delivery.

Opticians

Payment to opticians

Opticians send payment forms to Primary Care Support England. These include patient name, address, date of birth, whether an eye test was done, and the voucher issued. PCSE produces a statement for each optician which is sent to NHS England for payment. These statements do not contain personal data relating to patients.

Annual checklist

NHS England's local offices employ optometry advisors checking compliance of premises to delivery optical services. Compliance reports include the name of the practice owner.

Ophthalmic Post Payment Verification Process

Primary Care Support England provide NHS England with a report including name, date of birth and address of patients who have had a test, which is sent to the NHS England local office. The purpose of this is to identify ophthalmic contractor outliers and possible inappropriate claims for payment. Some payment forms and other data about the ophthalmic services you have received may be shared with NHS England and the NHS Business Services Authority where there is a need to investigate possible errors on the forms, payment errors or fraud.

Contracts

NHS England local offices hold contracts with opticians and information about applicants from new opticians. Application documents include correspondence, references, CVs, disclosure and barring checks and financial information.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'. For special categories (health) data the basis is Article 9(2)(h) – '…health or social care…'.

Specialised Commissioning

From April 2024 NHS England will delegate 59 Specialised commissioning services to the ICBs (detailed below) within three regions. These services will be jointly delivered, for this year (April 24-April 25).

NHS England East of England region

- Bedfordshire, Luton and Milton Keynes(BLMK) ICB
- Herts and West Essex ICB
- NHS Cambridgeshire and Peterborough ICB
- NHS Mid and South Essex ICB
- NHS Norfolk and Waveney ICB
- NHS Suffolk and North East Essex ICB

NHS England Midlands region

- NHS Birmingham and Solihull
- NHS Black Country
- NHS Coventry and Warwickshire
- NHS Derby and Derbyshire
- NHS Herefordshire and Worcestershire
- NHS Leicester, Leicestershire and Rutland
- NHS Lincolnshire
- NHS Northamptonshire
- NHS Nottingham and Nottinghamshire
- NHS Shropshire and Telford and Wrekin
- NHS Staffordshire and Stoke-on-Trent

NHS England North-West region

- NHS Cheshire and Merseyside
- NHS Greater Manchester
- NHS Lancashire and South Cumbria

For further detail on how commissioning is changing can be found on the NHS England website: NHS commissioning » How commissioning is changing (england.nhs.uk)

For details on integrated care: NHS England » What are integrated care systems?

For details on the commissioning road map: NHS England » NHS England commissioning functions for delegation to integrated care systems

Purposes for processing

Specialised services are accessed by comparatively small numbers of patients but with catchment populations of usually more than one million. They are provided in relatively few hospitals. These services tend to be located in specialised hospital trusts that can recruit a team of staff with the appropriate expertise and enable them to develop their skills.

The specialised services that we commission include Internal Medicine, Cancer, Mental Health, Trauma, Head and Spine, Women and Children, Blood and Infection, the Cancer Drugs Fund, high cost drugs and devices and Highly Specialised Services.

NHS England employs mental health case managers who are responsible for tailoring services to the individual requirements of mental health patients/clients. They work with professionals in provider organisations, sharing information to ensure that patients receive the best possible care in the most appropriate setting for their needs.

Sources of the data

The information may be collected from any organisation that provides specialised services to the NHS, including NHS Trusts and NHS Foundation Trusts, independent sector providers and charities.

Categories of personal data and recipients

NHS England uses data that has been anonymised in accordance with the Information Commissioner's Anonymisation code of practice, and summary data (numbers) for monitoring and payment for specialised services. This data is provided to us by NHS Digital who collects and analyses personal data submitted by providers on our behalf – see Data services for commissioners. The data processed by NHS Digital includes personal details such as NHS number, date of birth, postcode, and details of the diagnosis and treatment received.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For processing special categories (health) data the basis is Article 9(2)(h) '…health or social care…'.

Armed Forces and Families Health Care

Purposes for processing

The Armed forces Covenant is a promise by the Nation that those who serve or have served and their families are treated fairly. The Armed Forces Covenant is a part of the NHS Constitution. In relation to healthcare the Covenant states that the Armed Forces Community should enjoy the same standard of, and access to, healthcare as that received by any other UK citizen in the area they live and that Veterans should receive priority treatment where it

relates to a condition that results from their service in the Armed Forces, subject to clinical need.

NHS England commissions secondary care for serving personnel and Armed Forces families registered with MoD GP practices. It is also responsible for commissioning a range of services for veterans, such as those for limb loss and mental health.

Sources of the data

The information may be collected from any organisation that provides secondary health services to the NHS and the Armed Forces for serving personnel or their families, including NHS Trusts and NHS Foundation Trusts, Independent Healthcare providers, NHS and Defence GP Practices and other primary care providers and local authorities. Data may also be submitted by patients themselves and by other agencies to support the commissioning and ensure the delivery of packages of care.

Categories of personal data and recipients

NHS England uses data that has been anonymised in accordance with the Information Commissioner's Anonymisation code of practice, and summary data (numbers) for monitoring and payment for specialised services. This data is provided to us by NHS Digital who collects and analyses personal data submitted by providers on our behalf – see Data services for commissioners. The data processed by NHS Digital includes personal details such as NHS number, date of birth, postcode, and details of the diagnosis and treatment received.

Personal data may be submitted by patients themselves and by other agencies in relation to the commissioning individual packages of care.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'. For special categories (health) data the basis is Article 9(2)(h) – '…health or social care…'.

Health and Justice

Purposes for processing

NHS England is responsible for the routine commissioning of Health & Justice services. The current estate constitutes:

The Children and Young People's Secure Estate including

- Young Offender Institutions
- Secure Training Centres
- Secure Children's Homes
- Prisons (including Youth Offender Institutions)
- Immigration Removal Centres (IRCs)
- Public Health services for persons in detained and secure settings across England

We process personal data for our commissioning purposes, in order to conduct clinical reviews and conduct investigations into deaths in custody.

Sources of the data

The information may be collected from any organisation that provides health services to the NHS, including Prison Health care providers, NHS Trusts, NHS Foundation Trusts, and other health and justice care providers. Data may also be submitted by other agencies to support commissioning and ensure the delivery of individual packages of care.

Categories of personal data and recipients

NHS England uses data that has been anonymised in accordance with the Information Commissioner's Anonymisation code of practice, and summary data (numbers) for monitoring and payment for these services. This data is provided to us by NHS Digital who collects and analyses personal data submitted by providers on our behalf – see Data services for commissioners. The data processed by NHS Digital includes personal details such as NHS number, date of birth, postcode, and details of the diagnosis and treatment received.

Data that does not identify patients directly may be submitted by providers and other agencies in relation to the commissioning individual packages of care.

We also hold health care records in from prisons and other institutions within the secure estate. These records relate to prisons which have closed, or prisoners who have been released. The records document the care and treatment a prisoner has received. The records are held as they may become important, if there is a complaint or claim, which may typically be made months or years after the care received.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'. For processing special categories (health) data the basis is Article 9(2)(h) – '…health or social care…'.

NHS England is a joint data controller for records held on the system that we provide for prisons.

Secondary Care Dental

Purposes for processing

As part of its direct commissioning responsibilities, NHS England commissions all NHS dental services: primary, community and secondary care services, including dental hospitals and urgent dental care services.

The majority of specialist dental services are delivered in secondary care settings, in acute hospitals, foundation trusts, district general hospitals and (ten) dental hospitals funded by national and local tariff arrangements. Specialist dental services are listed below*, however some of these are recognised as multi-disciplinary care (dental and medical specialties). The definitions listed are in line with the General Dental Council:

- Special care dentistry
- Oral surgery
- Orthodontics
- Paediatric dentistry
- Restorative (endodontics, periodontics, prosthodontics, implant dentistry
- Oral medicine
- Oral microbiology
- Oral and maxillofacial pathology
- Dental and maxillofacial radiology;
- Oral and maxillofacial surgery

* Not all services are provided at every secondary or tertiary provider.

Sources of the data

The information may be collected from any organisation that provides health services to the NHS, including NHS Trusts, NHS Foundation Trusts, Dental Practices and other dental care providers.

Categories of personal data and recipients

NHS England uses data that has been anonymised in accordance with the Information Commissioner's Anonymisation code of practice, and summary data (numbers) for monitoring and payment for these services. This data is provided to us by NHS Digital who collects and analyses personal data submitted by providers on our behalf – see Data services for commissioners. The data processed by NHS Digital includes personal details such as NHS number, date of birth, postcode, and details of the diagnosis and treatment received.

Legal Basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For the processing of special categories (health) data the basis is 9(2)(h) '…health or social care…'.

Continuing Health Care – independent review panels

Purposes for processing

NHS Continuing Healthcare is a package of care for adults aged 18 or over which is arranged and funded solely by the NHS. It is available to individuals outside of hospital who have on-going health needs. This package is often delivered in an individual's own home or a care home. In order to receive NHS CHC funding individuals have to be assessed by Integrated Care Board (ICBs) according to a legally prescribed decision making process to determine whether the individual has a 'primary health need'. NHS England is required to establish arrangements for the independent review of ICB decisions on eligibility for NHS Continuing Healthcare funding.

An individual receiving care or their representative may apply for a review of an ICBs decision to decline funding by an NHS England Independent Review Panel. The independent review process is co-ordinated by the NHS Continuing Healthcare teams in each of the seven regions of NHS England.

Sources of the data

The personal data are submitted by the ICB and the applicant for review.

Categories of personal data

The information ICBs use to assess eligibility, and which may be submitted to an Independent Review Panel, fall under the following headings:

- behaviour
- cognition (understanding)
- communication
- psychological/emotional needs
- mobility
- nutrition (food and drink)
- continence
- skin (including wounds and ulcers)
- breathing
- symptom control through drug therapies and medication
- altered states of consciousness
- other significant needs

The obtained records that relate to these areas may include Care Home records, Health Records (for example GP, Hospital, Mental Health, District Nursing) and Social Care Records.

Categories of recipients

Personal data relating to the application is received by NHS England Continuing Healthcare teams and the members of the review panel. An Independent Review Panel is made up of:

- an independent chair
- a representative nominated by an Integrated Commissioning Board (not involved in the case);
- a representative from a Local Authority (not involved in the case); and
- at times there is also a clinical advisor in attendance.

Legal Basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'. For the processing of special categories (health) data the basis is Article 9(2)(h) – '…health or social care…'.

Individual Requests for funding

Purposes for processing

On an individual basis, there may be situations where a clinician believes that their patient's clinical situation is so different to other patients with the same condition that they should have their treatment paid for when other patients would not. In such cases, NHS clinicians can ask NHS England, on behalf of a patient, to fund a treatment which would not usually be provided by NHS England for that patient. This request is called an Individual Funding

Request (IFR). A guide for patients can be found on the NHS England website: NHS England » Individual funding requests for specialised services a guide for patients

Sources of the data

The information may be provided by a clinician who submits an IFR application form on behalf of a patient.

Categories of personal data

The IFR application form includes NHS number, name and address, date of birth, GP details, diagnosis, requested intervention and other information relevant to the request. Gender and ethnicity are also collected and held in anonymous form for equality monitoring.

Categories of recipients

Applications are considered by an independent panel who have not been involved in your treatment. The panel is made up of doctors, nurses, public health experts, pharmacists, NHS England representatives and lay members and is led by a lay chair.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'. For the processing of special categories (health) data the basis is Article 9(2)(h) – '…health or social care…'.

Payment for living kidney donation

Purposes for processing

NHS England reimburses people who donate organs (living donors) in order to ensure that the financial impact on the living donor is cost neutral. The principle of reimbursement is founded on the premise that there should be no financial incentive or disincentive in becoming a living donor. Living donors would usually submit a claim for financial reimbursement to NHS England in accordance with the NHS England published policy. The data submitted and processed allows for consideration of any claims and payment of expenses.

Categories of personal data

We collect this data from living donors to allow such reimbursement to take place. Data will include name, NHS Number and other personal details, and information about their stay in

hospital. Data may also include details of employment and income if claiming for lost income, including a letter from an employer, details of any other benefits you may be entitled to e.g. statutory sick pay.

Sources of the data

Hospital trusts; living donor co-ordinators; social workers; donor patients.

Categories of recipients

NHS England commissioning staff.

Legal Basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'. For the processing of special categories data the basis is Article 9(2)(h) – '…health or social care…'.

Data services for commissioners

Purposes for processing

Commissioning is the process of planning, agreeing and monitoring health services. It is not one action but many, ranging from the health-needs assessment for a population, through the clinically based design of patient pathways, to service specification and contract negotiation or procurement, with continuous quality assessment. NHS England and Integrated Care Boards (ICBs) are the commissioners that conduct these activities.

The Data Services for Commissioners programme has been established to improve NHS commissioning by ensuring that commissioning decisions, and the insights that support them, are based upon robust, standardised data that has been processed efficiently and is accessed legally.

For the purposes of this programme, the Secretary of State has directed NHS England to collect the personal data that we need from the organisations that we commission to provide health care.

Our analytical environments receive pseudonymised personal data which we analyse for our commissioning purposes.

Sources of the data

As a commissioner NHS England uses information from the providers of the services it commissions. These are:

- Specialised services
- Armed Forces and Families Health Care
- Health and justice
- Public Health Services
- Secondary Dental Services

Categories of personal data

For most commissioning purposes NHS England does not process data that identifies individuals directly. This is not necessary for our purposes. The purpose of the Data Services for Commissioners Programme is to enable us to analyse data for our commissioning purposes.

When NHS England collects personal data from providers of health care, the data includes information about the diagnosis, treatment received, postcode and date of birth. It also includes NHS number which is used to link data from several sources. An example of this is where we need information relevant to a Specialised Service, linked to the data submitted routinely by hospitals to NHS England via the Secondary Uses Service.

Categories of recipients

We provide anonymised and aggregate data (numbers) to ICBs and to the organisations that we commission to provide health care, or their data processors.

Legal basis for processing

For UK GDPR purposes NHS England's lawful basis for processing when directed by the Secretary of State is article 6(1)(c) – '…legal obligation…'.

This applies both to the collection and further processing of identifiable data under directions and to the processing of pseudonymised personal data for analytical purposes, under the Analytics Directions.

For the processing of special categories (health) data the conditions may be one or more of articles

9(2)(h) – '…health or social care…';

9(2)(i) – '…public health…'

9(2)(j) – '…statistical purposes…'.

Primary Care Support England

Purposes for processing

NHS England has a contract with Primary Care Support England to provide seven services as a data processor. These are described below.

Primary Care Records

PCSE provide a service to move hard copy patient records between GP Practices. They also store paper records for unregistered patients and the deceased. See Patients registered with GP Practices.

GP Payments and Pensions

NHS England is responsible for paying GP Practices for their services. The payments that PCSE administer are listed below with the type of data and sources.

Payment type	Data type	Source
Global sum payments	• GP Name • GD Code • Practice Code	Registration list (NHAIS)
PMS contract baseline payments	• Practice Code	Registration list (NHAIS) and contract variation template from Regional Local Team/CCG
Drugs payments (prescribing and dispensing)	• Practice Code • Partnership details / code • GP Names • GD Code	NHS Digital dependency
Childhood immunisations payments	• Practice Code • GP Name • GD Code	Open Exeter
Seniority payments	• Partnership details / code	Performer list/NHAIS

	• DoB • Sex • National Code • GMC Number • Country of Birth • Start date • Registered date • Length of service • Share / salary details	
Ad-Hoc payment instructions (Locum/Premises/Rates)	• Practice Code	RLT/Delegated CCG
GP trainee payments and expenses (For non-lead employer areas)	• Registrar Name • Practice Code • GMC Number • Partnership Code • Trainer Name • CTP Date	Health Education England / Practices
GP training grant payments	• Registrar Name • Practice Code • GMC Number • Partnership Code • Trainer Name • CTP Date	Health Education England / Practices/RLT's for non lead employer areas
Enhanced Service payments via CQRS	• Practice Code	Extracted from GP practice systems by NHS Digital acting under directions.
Quality and Outcomes Framework payments (aspiration)	• Practice Code	NHS Digital direct dependency
Quality and Outcomes framework payment (achieved)	• Practice Code	Extracted from GP practice systems by NHS Digital acting under directions.
Public Health Immunisation Schedules payments	• Practice Code	RLT/Delegated CCG
GP retainers	• Practice Code	HEE / Local area teams
Local Medical Committee levies-depends on contract type	• Practice Code • CCG Code	LMC/NHSE

PCSE also act as the administrator for GP pensions on behalf of NHS England. The pension and its funds are managed by NHS Pensions and not PCSE. Any decisions related to the management of a pension are the responsibility of NHS Pension and / or NHS England, PCSE are only responsible for the administration element which includes processing forms / documentation and allocating funds to account.

As part of this process, PCSE may collect personal identifiable information relating to members of the pension, including name, address, date of birth, national insurance number and salary details. If you have an enquiry regarding what personal identifiable information is processed as part of the pensions administration, you may contact PCSE at Contact us | PCSE (england.nhs.uk)

Pharmaceutical List – market entry applications

Pharmaceutical lists are maintained by Integrated Care Boards and all market entry applications for inclusion in a pharmaceutical list are made to pharmacy contract teams. The National Health Service (Pharmaceutical and Local Pharmaceutical Services) Regulations 2013 as amended provides the regulatory framework for maintaining pharmaceutical lists. Applications for inclusion in a pharmaceutical list must be made by sending NHS England an application in line with these regulations.

The personal data collected includes; full name, sex, date of birth, residential address and telephone number. For further information please refer to the Pharmacy Manual – List of Annexes.

NHS England's policies and procedures for managing pharmaceutical services, providers and the lists are set out in the Pharmacy Manual.

Primary Care Support England (PCSE) is responsible for administering applications for inclusion in a pharmaceutical list on behalf of Integrated Care Boards.

Ophthalmic payments

Opticians send payment forms to Primary Care Support England. These include patient name, address, date of birth, whether an eye test was done, and the voucher issued. PCSE produces a statement for each optician which is sent to NHS England for payment. These statements do not contain personal data relating to patients.

Performers Lists

There are three National Performers Lists operated by NHS England – one for medical, dental and ophthalmic performers. The lists provide an extra layer of reassurance for the public that GPs, Dentists and Opticians practicing in the NHS are suitably qualified, have up

to date training, have appropriate English language skills and have passed other relevant checks such as with the Disclosure and Barring Service (DBS) and the NHS Litigation Authority.

PCSE administer initial entry to the National Performers List. The decision to admit or decline an applicant to the National Performers Lists is the responsibility of NHS England. PCSE also administer changes to a performer's status, transfers between practices (for medical performers only) and performer movement between local teams on behalf of NHS England.

As part of this process, PCSE collects personal data, as detailed via information collated on NHS England's official national performers lists documents, please see www.performer.england.nhs.uk. If you have an enquiry regarding what personal information is processed as part of the performers lists, please email pcse.performerlists@nhs.net.

Open Exeter

Open Exeter is a facility to enable access to the list of patients registered with GPs that is held by NHS Digital on behalf of NHS England. PCSE administer the authorisation process for access and issue access credentials. Access by organisations is approved by NHS England's Caldicott Guardian.

Practice Mergers and Closures Notifications

PCSE are responsible for administering and updating systems when advised of GP practice closure and merger, on behalf of NHS England. This process includes transferring between/removing GP's from practices.

As part of this process, PCSE collects personal data, as detailed on NHS England's official NPL3 document, please see www.performer.england.nhs.uk. If you have an enquiry regarding what personal information is processed as part of the performers lists, please email pcse.performerlists@nhs.net.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'. and Article 6(1)(c) '…legal obligation…'. For purposes relating to GP payments and pensions the lawful basis for processing is Article 6(1)(b) – processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

For the processing of special categories (health) data the basis is Article 9(2)(h) – '…health or social care…'.

Legacy records

Purposes for processing

Legacy records from Primary Care Trusts (PCTs) and Strategic Health Authorities (SHAs) were transferred to successor organisations as part of a legal transfer in 2013. This work was led by Department of Health. Departments within NHS England that are now responsible for a particular function received the records and information that they required for the function to progress within this transfer.

The NHS England Records Management Team is responsible for the management of closed legacy records. These paper legacy records are stored securely all over the country with 23 suppliers and are available to teams if needed for business needs. The personal data in these records may be provided in response to subject access requests and is subject to the other GDPR rights.

Categories of personal data

The categories of legacy records that we hold are as follows:

- Audit/Clinical Audit
- CAMHS (Child and Adult Mental Health Services) / Children's and Young Persons Service/Family Planning Clinics and Services
- Clinical i.e. specialist commissioning / performance management / Serious Untoward Incidents
- Complaints/PALS
- Dental (includes patient records)/ Dental GP Contracts / Emergency Dental Service
- Enhanced Services
- Estates Management
- GP Appraisals [deregistered and RIP GP patient files held by PCS]
- Incidents (including infection prevention and control)
- Legal claims/issues
- Management and use of Controlled Drugs / Medicines Management / Medical Director
- Mental Health Commissioning
- Nursing and Quality - Safeguarding
- PEC (Professional Executive Committee)
- Primary Care Commissioning and Contracting - Dental/GP/Director/Medical/Medicines Management/Pharmacy/Optometry/Non Acute Commissioning/Non Funded Care/Extra Contractual Referral
- Quality and Clinical Governance
- Safety and Quality

- Ophthalmology (payments)

Many but not all of these records include personal data.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'. For the processing of special categories (health) data the basis is Article 9(2)(h) – '…health or social care…'.

Evaluation of the Targeted Lung Health Check programme

Purposes for processing

The Targeted Lung Health Checks (TLHC) programme is a new and ground-breaking flagship programme of work in England which will contribute to the ambition of the NHS Long Term Plan to improve early diagnosis and survival for those diagnosed with cancer.

The TLHC programme targets those most at risk of lung cancer and will work with Integrated Care Boards (previously CCGs), who have some of the highest rates of mortality from lung cancer. The programme will work with initially ten projects, but then expand to other Integrated Care Boards across England to deliver the programme. It is expected that this programme will run Nationally, covering all areas of England from 2024 onwards.

People aged over 55 years old but less than 75 years old that have ever smoked will be invited to a free lung check.

Following the lung health check those assessed as high risk will be offered a low dose Computerised Tomography (CT) scan.

NHS England is conducting a national evaluation to understand the impacts and economics of the programme. The evaluation is expected to demonstrate impacts on patient health outcomes, experience and wider health inequalities. Findings from the evaluation will ensure an evidence-based approach to NHS
targeted screening programme of this kind.

This approach involves an analysis of data collected by the programme, and information recorded in interviews with patients and staff about their experiences.

Ipsos, together with the Strategy Unit at the Midlands and Lancashire Commissioning Support Unit (CSU), which is part of NHS England, have been appointed jointly as our national evaluation partner.

Ipsos will conduct telephone interviews with people who have agreed to be contacted and produce anonymous findings from those interviews.

More information about how data will be used by NHS England to evaluate its Cancer Referral Services is in their general privacy notice and its Cancer Programme Pilots Evaluation privacy notice.

Sources of data and categories of personal data

Integrated Care Boards coordinate the TLHC service locally acting for their constituent GP practices. Participants are invited for a lung health check by their Integrated Care Board, or constituent GP practice, before being referred into secondary care for further investigations and treatment (where necessary).

Personal data about participants is collected across the pathway by Integrated Care Boards to enable the delivery of the TLHC service to patients locally.

The national evaluation partner receives a data set from the Integrated Care Boards for the purpose of evaluation. Participants will not be identifiable from this dataset. The dataset will include information on sex, age, marital status, main language, occupation, information about diagnosis, treatment and outcomes. You can read more about how your data will be evaluated and our legal basis to process as part of the Cancer Programme Pilots Evaluation notice: NHS England » Cancer Programme Pilots Evaluation (England): transparency notice

The evaluation partner will also collect information about the experiences of participants and staff who have consented to be contacted, facilitated by the local Integrated Care Boards. Information will be recorded in a way to ensure that individuals cannot be identified.

Categories of recipients

As detailed in the Cancer Pilots Evaluation privacy notice.

Ipsos also collects information through interviews with people who have consented to being contacted, which will be anonymised before sharing with NHS England. Ipsos acts as a processor for NHS England for the purposes of the evaluation.

Participants Experience Interviews

You might have been asked by your local targeted lung health check programme run by the Integrated Care Board on behalf of your GP if you would like to feedback on your experience of the Targeted Lung Health Check programme as part of the service evaluation. In agreeing to this, the personal information we process is provided to us directly by you for the following reason:

- To invite you to participate in an interview for the evaluation

- To evaluate the TLHC programme

Where you have consented to take part in the survey or an interview, NHS England will collect and process the following information for the purposes of the interview:

- Name and contact information
- Age band
- Gender
- Ethnicity
- Religion
- Smoking status and intensity
- Previous engagement with the TLHC programme
- Your responses to interview/focus group

We will not keep any of your personal data collected as part of the survey or interview. Once your responses have been collated, your personal information will be anonymised.

Staff Interviews

The personal information we process is provided to us directly by you for the following reasons:

- Invite you to participate in an interview for the evaluation
- To evaluate the TLHC programme

With your consent NHS England will collect and process the following information for the purposes of the interview:

- Name and contact information
- Your feedback to interview/focus group

We will not keep any of your personal data collected as part of the survey or interview. Once your responses have been collated, your personal information will be anonymised.

Legal basis for processing for the purposes of patient experiences

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…';

For the processing of special categories (health) data the basis is 9(2)(h) – '…health or social care…', and 9(2)(j) '…statistical purposes…'.

Those taking part in the Community Pharmacy Consultation Service for people attending Emergency and Urgent Care with a minor illness

Purposes for processing

NHS England is testing a new service in community pharmacies to offer people a consultation service for people who have attended urgent or emergency care with a minor illness or who need an urgent repeat prescription. Midlands and Lancashire Commissioning Support Unit (part of NHS England) are working with NHS England to evaluate this new service in local community pharmacies. The pilot aims to understand what works well, and less well and, if necessary, how it might be improved in the future.

Midlands and East Lancashire Commissioning Support Unit will host a survey and conduct telephone interviews with people who have agreed to be contacted to be invited to take part.

Sources of data and categories of personal data

In order to find out if this new service is working well, we will need to process information about you. Most of this information will be collected by the pharmacist when providing you with the service and shared with to Midlands and Lancashire Commissioning Support Unit which is part of NHS England (see below). This will include information about your consultation but no information that identifies you.

You will have been asked at your referral whether you agree to be contacted and where you have agreed, we will ask you take part in a very short text message survey after your consultation with the pharmacist so you can tell us about your experience of this service. We may also ask you take part in a telephone interview.

Midlands and Lancashire Commissioning Support Unit (part of NHS England) are carrying out this evaluation on behalf of NHS England. Their privacy policy can be found found on their website.

How will NHS England use any personal data including your responses?

NHS England will use your personal data and responses solely for evaluation purposes and to produce findings and insights for NHS England in relation to this new service.

If you agree, we may use your mobile phone survey to send you a customer satisfaction survey by text and we may also contact you with a request to undertake a telephone interview. If you do take part in a telephone interview at a later date, your answers will be collected using digital recorders, note-taking, and in some cases, the sound files will be used to produce transcripts. The sound files will be destroyed as soon as the transcripts have been undertaken.

How long will NHS England retain my personal data and identifiable responses?

NHS England will use your personal data and survey/interview responses solely for evaluation purposes and to produce findings and insights for NHS England in relation to this new service.

We will not keep any of your personal data collected as part of the survey or interview. Once your responses have been collated, your personal information will be anonymised.

If you agree, we may use your mobile phone survey to send you a customer satisfaction survey by text and we may also contact you with a request to undertake a telephone interview. If you do take part in a telephone interview at a later date, your answers will be collected using digital recorders, note-taking, and in some cases, the sound files will be used to produce transcripts. The sound files will be destroyed as soon as the transcripts have been undertaken.

How long will NHS England retain my personal data and identifiable responses?

NHS England will only retain your personal data in a way that can identify you for as long as is necessary to complete the evaluation. In practice, this means that once we have satisfactorily reported the anonymous research findings to NHS England, we will securely remove your personal, identifying data from our systems.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…';

For the processing of special categories (health) data the basis is 9(2)(h) – '…health or social care…'

Other Information

This information sheet is about how we will use your personal data for the the purposes of the survey and telephone interview, your personal data collected as part of the evaluation will be anonymised and not shared with any other person or organisation.

Your pharmacy must also separately share limited information with other NHS bodies regarding the services they deliver, including with NHS England who have commissioned the referral service. Please also see your pharmacy's privacy notice to understand how they will use your information. More information about how your data will be used by NHS England to evaluate its Cancer Referral Services is in their general privacy notice and its Cancer Pilots Evaluation privacy notice.

Maternity and Neonatal Independent Senior Advocacy (MNISA) - Privacy Notice

Information Commissioning Boards (ICBs) and NHS England are working together to deliver the MNISA service (a list of all ICBs involved in this pilot can be found below).

For the purposes of data protection laws, the ICBs and NHS England are “joint controllers” for the use (processing) of your personal information in this notice. This means that we have both worked together to decide why and how your personal data (processed). It also means we are jointly responsible to you under the law for that processing.

To confirm:

- The ICB in your pilot area is responsible for handling your personal information regarding any engagement you have with the MNISA service
- NHS England has responsibility for providing the reporting system that the MNISA service (e.g., an ICB) uses to handle your personal information. For example, securely storing any information you provide when engaging with the service. NHS England will also process your de-identified and anonymised data to ensure the service works, can improve and adapt to any changing requirements

This notice describes how and why your personal information is used and by who. Any sharing of that information; by who and why. As well as how to contact us or NHS England should you have any questions or concerns about the use of your personal information.

Whilst the ICBs and NHS England are joint controllers for your information. The ICBs have taken responsibility to be the point of contact for any data protection queries. Please see your local ICB privacy notice for information around how they process your personal data for this pilot service.

The type of personal information we collect

We collect and process the following information:

- Your contact information; name, telephone number, email address
- Health related information
- Date and details relating to your experiences
- Racial or ethnic origin

How we get the personal information and why we have it

The personal information is provided directly by you for one of the following reasons:

- When you approach the MNISA service to engage with an Advocate/the service
- NHS England use your personal data to assess the viability of the service and ensure improvement in services; for both the MNISA and maternity services
    - This includes using de-identified information to help understand themes and trends raised, scope and reach of the service, to be able to report progress of the pilot and to help understand the impact of the MNISA work.

Under the UK General Data Protection Regulation (UK GDPR), the lawful bases the ICBs and NHS England rely on for processing your information under this service, and of which is special category data are:

- Article 6(1)(e) We need it to perform a public task.
- Article 9(2)(h) We need it for the provision and management of our health or social care system

How we store your personal information

Your personal information is stored securely on NHS England's, IT system. Your personal information will not be routinely accessed by anyone in the ICBs or NHS England, apart from the MNISA themselves and relevant staff (e.g., line management for business continuity purposes or in cases where your advocate is absent and your case, with your agreement, is transferred accordingly) or in the event of a technical issue with CRM and it is necessary for NHS England to assess the issue to maintain the security and functionality of the system and its data.. We and NHS England will retain and dispose of your personal information in line with the NHSX_Records_Management_CoP_V7.pdf (england.nhs.uk).

Your data protection rights

Under data protection law, you have a number of data protection rights. For example, right of access, where you have the right to ask us for copies of your personal information. You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

The regulatory body responsible for upholding data protection, the Information Commissioner's Office (ICO) also has information regarding data subject rights which can be found here: A guide to individual rights | ICO

Please contact your local pilot ICB if you wish to make a request.

List of ICBs involved in the pilot:

1. Bath and North East Somerset, Swindon and Wiltshire
2. Birmingham and Solihull
3. Cheshire and Merseyside
4. Cornwall
5. Devon
6. Frimley
7. Gloucestershire
8. Kent and Medway
9. Lancashire and South Cumbria
10. Leicester, Leicestershire and Rutland
11. Mid and South Essex
12. North East London- External
13. North Central London
14. North East and North Cumbria- External
15. Nottingham and Nottinghamshire
16. Shropshire, Telford and Wrekin

17. Somerset
18. South Yorkshire
19. Staffordshire and Stoke on Trent
20. Suffolk and North East Essex
21. West Yorkshire

Evaluation of the Rapid Diagnostic Centres

Purposes for processing

The rollout of Rapid Diagnostic Centres (RDCs) across England is designed to speed up diagnosis of cancer and other serious conditions.

RDC pathways make sure everyone with suspected cancer gets the right tests at the right time in as few visits as possible. Driving innovation and new diagnostic practice, RDC pathways promote continuous improvement of cancer diagnostics.

The service provides:

- Coordinated access to a diagnostic pathway for all patients with symptoms that could indicate cancer
- A personalised, accurate and rapid diagnosis of symptoms by bringing existing diagnostic capabilities and clinical expertise together

RDCs also introduce a new non-specific symptom pathway for patients who display symptoms that could indicate cancer that don't align to specific cancers, such as unexplained weight loss, fatigue or vague abdominal pain. The new non-specific pathway complements current cancer diagnostic pathways, as well as providing elements that can be applied to existing pathways.

By 2024 the programme will achieve full population coverage across England for non-specific symptom pathways and be applying the RDC pathway principles to every site-specific symptom pathway

NHS England has commissioned independent partners Ipsos MORI and York Health Economic Consortium (YHEC) as processors, in collaboration with the Strategy Unit at Midlands and Lancashire Commissioning Support Unit (CSU – part of NHS England) to undertake a comprehensive evaluation of the RDC programme. The evaluation will provide ongoing feedback to inform the delivery of RDC pathways and the strategic direction of the programme.

The evaluation will use mixed quantitative and qualitative methods to assess the processes, impact, and economics of RDC pathways to understand:

- Patient experience and impacts on the health and care system
- The best approach to delivering national pathways for specified cohorts of patients;
- What pathway changes are optimal, in what context(s)
- How patients move through RDC pathways and the outcomes they experience as a result by analysing the impact of RDC pathways on metrics such as waiting times and cancer staging
- The cohorts of patients being referred into RDC pathways and the sequences of tests performed to enable continuous improvement of the services

The initial evaluation will include:

- A sampled experience of care survey
- Qualitative interviews with patients and RDC programme staff
- Case studies of selected RDC pathways
- An economic survey and evaluation
- An impact evaluation using a collation of patient level data through a newly developed Trusted Research Environment for Cancer hosted by NHS Digital

Sources of data and categories of personal data

Patient Level Personal Data is obtained from the datasets held in the National Disease Registration Service - see National Disease Registration Service: NHS Digital Transparency Notice - NHS Digital for further information.

Patient Level Personal Data is obtained from NHS Digital held commissioning datasets for Cancer Waiting Times (CWT), National Cancer Registration data and the Rapid Cancer Registration data, Hospital Episodes Statistics (HES), and Civil Registration dataset.

Patient Level Personal Data is submitted by RDC's to the National Cancer Registry and Analysis Service (NCRAS). The minimum dataset includes

- Cancer Alliance Code
- Provider Code
- NHS Number
- Date of birth
- Health information
- Diagnosis information

- Testing information

Data is obtained directly from Patients and Staff who agree to provide responses to care surveys and qualitative interviews.

Categories of recipients

Ipsos Mori, the Strategy Unit at the Midlands and Lancashire CSU and the York Health Economic Consortium, will process a linked dataset of pseudonymised personal data provided by NHS Digital under a Data Sharing Agreement with NHS England that will enable the evaluation processors to analyse data within a trusted research environment.

Ipsos Mori also collects information through surveys and interviews, which will be anonymised before sharing with NHS England. All of the outputs from the evaluation will be provided in an anonymised form to share with NHS England and the Cancer Alliances.

Legal basis for processing

NHS England's lawful basis for processing the data is Article 6(1)(e) – '…exercise of official authority…'

For the processing of special categories (health) data the basis is 9(2)(h) – '…health or social care…'.

For the processing of the Patient care and staff surveys and interviews, explicit consent will be relied upon in order to obtain the required information.

NHS Wayfinder Services

About this privacy policy

NHS England provides the Wayfinder services that enable people and carers to access information about their secondary care referrals and their elective care via the NHS account (either the NHS App or nhs.co.uk).

This privacy policy explains how NHS England and other organisations may use your data for this purpose.

Data Controller's Contact Details

The Secretary of State has issued directions to NHS England to deliver Wayfinder. The legal direction is titled Wayfinder Services Directions 2023, dated 5 July 2023.

NHS England are joint controller with the Secretary of State for the data we need to provide the Wayfinder services unless otherwise stated.

NHS England are also joint controller, with the Secretary of State for the NHS App. Please visit the NHS App webpage for further details.

Please visit the NHS England website for contact details.

Our purpose for using your data

We use your data to help you access information about secondary care referrals and your elective care via the NHS App. We will do this by integrating Patient-Facing Systems (also known as personal health record (PHR) services) with the NHS App to provide more patient-centered care at local and national levels.

Our aims are to:

- Create a better experience for you, so you have more control over your care.
- Be able to give more people more access.
- Be able to give you information relevant and tailored to you.
- Reduce the number of paper letters sent by post.
- Reduce our carbon footprint.
- Reduce waiting times and decrease waiting lists
- Make a positive contribution towards the Elective Care Backlog Recovery Programme and its goals

In using your data, we will be able to do the following in the NHS App, both in mobile and desktop formats:

- Present you with information on:
    - Referrals and their status
    - Future and historical hospital appointments
    - Clinical Documents including things such as appointment letters, outcome letters, discharge summaries, etc.
    - Questionnaires relevant to your hospital care
    - Patient test results and other such patient-facing clinical data sources
    - Wait list information and average wait times
- Send you notifications and messages regarding the above information
- Enable you to access
    - e-RS, to book your initial outpatient appointment
    - Patient-Facing Systems, to book, change and cancel appointments
- Provide a way for you to provide feedback
- Provide a way to collect and analyse data to improve services.

This service does not include profiling or any automated decision making.

Where do we get information from?

We collect data from NHS Trusts via their Patient Facing Systems as well as other areas of NHS England as explained below:

Role	What is it?	Data Controller
Patient-Facing System	This enables you to manage your appointments, view important documents and complete questionnaires.	Trusts
e-RS **(Electronic Records Service)**	National e-Referrals Service provides information about your referrals and appointments. Integrated with aggregator for appointment data and allows deep links into existing Manage Your Referral functionality	NHS England
Waiting List Minimum Data Set (WLMDS)	Wait time data source system managed by NECS. Wait time data source system, processing anonymous WLMDS data in order to return average wait time information per speciality in each Trust. Collates and processes latest waiting list data provided by Trusts, making it available to consume and surface wait time information to patients within the NHS App. Data provided at patient level (NHS number) enabling patient to be identified to surface relevant average waiting time information.	NHS England

Data we collect about you

Data Categories	Why do we need this?
Personal Data	
NHS Number	Your NHS Number is part of your Personal Medical Record and is used for matching and validation.
Surname	This is part of your Personal Medical Record and is used for matching and validation.
Name	This is patient contact information that is part of your Personal Medical Record and used to help our service desk resolve any user issues.

Date of Birth	This is part of your Personal Medical Record and is used for matching and validation.
Email Address	This is patient contact information that is part of your Personal Medical Record and used to help our service desk resolve any user issues.
Phone number	This is patient contact information that is part of your Personal Medical Record and used to help our service desk resolve any user issues.
Special Category Data	
Appointment data E.g. appointment identifier, appointment date, appointment location, appointment type / description	We need this to: - be able to present appointment information to you. - help our service desk resolve any user issues.
Referral data E.g. referral identifier (UBRN), referring organisation (ODS Code and name), referral status	We need this to be able to present referral information to you.
Document data E.g. document type, document status	We need this to be able to present documents to you.
Questionnaire data E.g. questionnaire type, questionnaire status	We need this to be able to present questionnaires to you.
Patient-specific wait times data E.g. patient presence on waiting list	Required to link this data with other sources e.g. WLMDS, in order to surface average wait time data relevant to the patient (based on specific e.g. speciality, trust, etc.).
Test results	Required to surface patient clear and navigable test result information to patients.
Condition / pathway data E.g. SNOMED code for a patient's condition	Required to enable delivery of a tailored patient experience related to their individual condition or care pathway.
Speciality	Required to deliver relevant information to patients based on the speciality.

Messages from health and care providers E.g. new appointment containing key information such as location, speciality, clinician name etc.	Required to update patients on their care and required actions. Messages processed as part of NHS App Messaging and NHS App Notification Services will persist within the NHS App repositories.
Non-Personal Data	
Portal URL (deep link)	Required to allow patients to access Wayfinder content and features delivered via Patient-Facing System within NHS login-enabled experience.
Portal identifiers e.g. NHS login, eRS or Patient-Facing System identifiers	Required to connect together patient information across different systems via pseudonymised identifiers.
Wait times rolled-up data	Aggregated dataset (e.g. for Trust, speciality, procedure) required to match with patient presence on wait list (from WLMDS) to provide wait time information relevant to the patient.
Patient analytical data E.g. overall number of patient logins to Wayfinder, number of unique patient logins to Wayfinder	Data about patient interaction with Wayfinder functionality gathered by a Management Information Reporting Service in order to inform business case benefits mapping, Key Performance Indicators (KPI) / Management Information (MI) generation and service delivery improvement opportunities. Will in some scenarios require processing of patient Personal Data (e.g. NHS Number) in order to generate pseudonymised data at a per patient level.

Do we share any of your information?

NHS England may share data back to the NHS Trust which originally provided it, in identifiable or pseudonymised form, at the request of the NHS Trust to assist in resolving any technical or quality assurance issues.

Anonymous and summarised data will be shared with NHS Trusts, commissioners & policy teams at national, regional and provider level to support strategy and operational decisions and with Department of Health and Social Care and its associated bodies (NHS England, UK Health Security Agency etc.) to support service delivery.

Anonymous and summarised data may also be shared to support research and audit.

Where do we store your information and how long do we keep it for?

We only store and process your personal data within the UK and European Economic Area (EEA).

Your information is stored as follows:

Category of information	Retention period
Personal Data	Your NHS numbers is held forever in order for you to be able to access all historical Trust healthcare information. The service caches the NHS login ID token (which contains NHS Number, surname and data of birth) to support the user with a seamless authentication journey between services that will be retained in a local cache only for the duration of the user session. Database transaction logs, record locators, infrastructure access logs, edge logs and application logs are retained within the programme; redacted logs sent to the Cyber Security Operation Centre (CSOC) in line with the CSOC retention policy. - Database transaction logs – 5 years - Record locators – 40 days - Infrastructure access logs – 40 days - Edge logs – 40 days - Application logs – indefinitely
Special Category Data	Audit Logs are retained for 5 years. All other data is pass-through i.e., relayed to a subsequent target system from the sending source system.
Non-Personal Data	Audit Logs evidencing message processing are retained for 2 years. Audit logs evidencing events processing are retained for 15 months. Audit logs evidencing access are retained for 40 days. All other data is pass-through i.e., relayed to a subsequent

	target system from the sending source system.
Reporting Data	MI Reports are retained for 5 years, and MI events are retained for 5 years for analytical purposes in line with the 5 year duration of benefits forecast in the Wayfinder Business Case. Data will be held in pseudonymised form. Audit logs evidencing access & review are retained for 40 days

Our Legal basis for processing

The UK General Data Protection Regulation (UK GDPR) sets out the requirements on organisations who collect and process personal data from people in the UK. Where NHS England processes personal data, we need to comply with the UK GDPR.

Having a legal direction in place puts NHS England under a legal obligation to comply with this requirement and so meets Article 6(1)(c) of the UK GDPR. To deliver certain parts of the NHS App, such as when we are using your cookies, we also need your consent so meeting Article 6(1)(a) of the UK GDPR.

Your health data has extra legal protection and NHS England must also comply with Article 9 of the UK GDPR. To process your health data, we rely on:

- Article 9(2)(g) of the UK GDPR which applies where there are "reasons of substantial public interest". The Department of Health and Social Care has decided that it is in public interest for NHS England to provide the NHS App to the public. In addition, Schedule 1, Part 2 paragraph 6 of the Data Protection Act 2018 in relation to statutory and government purpose.
- Article 9(2)(h) of the UK GDPR which applies as your NHS App supports the provision of health and social care to you. In addition, Schedule 1, Part 1 paragraph 2 of the Data Protection Act 2018 in relation to a health or social care purpose.

What are your rights?

You have a right to:

- know how and why your data will be collected, processed and stored
- request a copy of your personal data
- correct errors or omissions in your personal data
- to ask us to restrict our use of your personal data (for example, if you think it's inaccurate and needs to be corrected)

You can exercise your rights by contacting the relevant controller.

For data held and processed by NHS England, please visit the NHS England website for contact details.

If you wish to exercise your rights regarding data held and processed by your hospital, please get in touch with your hospital using the contact details in the hospital's privacy policy, published on their website.

How do you complain?

If you have any objections or complaints relating to your data, we will investigate and attempt to resolve them. We will make every reasonable effort to allow you to exercise your rights as quickly as possible and within the timescales set out in data protection laws.

You can contact our Data Protection Office at NHS England to make a complaint. You can do this by emailing enquiries@nhsdigital.nhs.uk or by sending a letter to:

Privacy Transparency and Ethics team
7 and 8 Wellington Place
Leeds
West Yorkshire, LS1 4AP

We ask that you try to resolve any issues with us first. However, you have a right to lodge a complaint with the Information Commissioner's Office (ICO) at any time about our processing of your personal information. The ICO is the UK regulator for data protection and upholds information rights. Contact the ICO.

Cancer Programme Pilots Evaluation (England): Transparency Notice

This transparency notice explains for the Cancer Programme Pilots Evaluation:

- Why we collect information about you (we call this "**personal data**").
- What we do with it, including who we share it with.
- How long we keep it for and where we store it.
- Our legal basis for using it.
- What your data protection rights are.

This notice covers the data we collect for the Cancer Programme Pilots from health care services in England.

This notice should be read in conjunction with the NHS England General Privacy Notice. To read more about how NHS England uses personal data to improve health and care, see Transparency Notice: how we use your personal data.

About the Cancer Programme Pilots Evaluation:

The NHS Long Term Plan (LTP) was published in January 2019. It sets out stretching ambitions and commitments to improve cancer outcomes and services in England over the next ten years. The key ambitions in the NHS LTP for cancer are:

- by 2028, 55,000 more people each year will survive their cancer for five years or more; and
- by 2028, 75% of people with cancer will be diagnosed at an early stage (stage one or two).

The NHS Cancer Programme continues to support the recovery of cancer services, funding Pilots to lead change at the local level through Cancer Alliances, who work in collaboration with their local Sustainability and Transformation Partnerships (STPs), Integrated Care Boards (ICBs) and their Integrated Care Systems (ICSs).

The Cancer Programme collects data on all their pilots (Cancer Pilots) for monitoring and evaluation purposes, as they need to understand how effective their Pilots are individually and together for creating changes to benefit patients, such as improving earlier diagnosis and survival of cancer.

It is expected that the data collected will be used to evaluate a number a Cancer Pilots, together and individually. Those which are currently being evaluated are:

- **Community Pharmacy Pilot** – NHS England » Those taking part in the Community Pharmacy Consultation Service for people attending Emergency and Urgent Care with a minor illness
- **Targeted Lung Health Check** (**TLHC**) – NHS England » Evaluation of the Targeted Lung Health Check programme

Where we get your data from

For Cancer Programme Pilots, we collect data from health care providers in England who have been commissioned by NHS England to deliver the Pilots.

Data is submitted securely to NHS England. These organisations are legally obliged to provide NHS England with the information as set out in the Cancer Programme Pilot Evaluation Data Provision Notice issued to them under section 259(1)(a) of the Health and Social Care Act 2012.

For current Pilots we collect data from:

- Community Pharmacies in England who are participating in the Community Pharmacy Pilot, as set out in Annex A of the Data Provision Notice
- Targeted Lung Health check sites in England, who are participating in the TLHC Pilot As set out in Annex B of the Data Provision Notice

How we use your data

We will de-identify your data and use your de-identified data to determine the outcomes of patients referred through the Cancer Programme Pilots, which is necessary to evaluate the safety and effectiveness of these Pilots.

The de-identified data is linked to other data NHS England already holds about your care and treatment which is held in other national data datasets we collect. This includes:

- Data in the Cancer Outcomes and Services Data Set. This is data about information required to support national cancer registration and associated analysis (at local, regional, national, and international level), as well as other national cancer audit programmes.
- Data in the Cancer Waiting Times Data Collection . This is data about information collected from providers of NHS cancer care to calculate and monitor performance against nationally set cancer targets for referrals, diagnosis and treatment.
- Data in the Hospital Episode Statistics. This is data about admissions, outpatient appointments and historical Accident and Emergency attendances at NHS hospitals in England.

The linked de-identified data will also be analysed to produce anonymous aggregate management information reports which will not identify any individuals.

Our role

Under data protection law, NHS England is the ‘controller’ for the Cancer Programme Pilot data collections. This means that we make decisions about what personal data we need to collect and how we will use your data to run the data collection. More information about our legal basis to process your data is in the ‘Our Legal Basis’ section below.

Our legal basis

NHS England is required to have a legal basis under data protection law to collect and process your personal data to evaluate the Cancer Pilots.

Under UK GDPR, NHS England is the joint controller of your data with the Secretary of State for Health and Social Care with regard to the establishing the purposes of the Cancer

Programme Pilots Evaluation. NHS England is sole controller in respect of processing your personal data.

Our legal basis is:

Legal obligation - Article 6(1)(c) of UK GDPR. This is because the Secretary of State for Health and Social Care has issued NHS England with Directions under section 254 of the Health and Social Care Act 2012 to collect and analyse Cancer Pilots data. These Directions are called the Cancer Pilots Evaluation Directions 2024

We also need an additional legal basis in the UK GDPR and the Data Protection Act 2018 (DPA 2018) to process special categories of personal data, which includes data about your health. Our legal bases to use data relating to your health for the purposes of the Cancer Pilots are:

- GDPR Article 9 (2) (g) - processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. DPA 2018 Schedule 1, Part 2 (6) (2) (a) Statutory etc and government purposes – the processing is necessary for the exercise of a function conferred on a person by an enactment or rule of law and is necessary for reasons of substantial public interest; and/or
- Article 9 2 (h) Processing is necessary for the provision of health care or treatment, and for the management of health care systems or services, supplemented by DPA 2018, Schedule 2, Part 1, paragraph 2 health and care purposes; and/or
- Article 9(2)(i) – public interest in the area of public health, supplemented by DPA 2018, Schedule 1 Part 1, paragraph 3 - public health; and/or
- Article 9(2)(j) processing is necessary for Research and statistics supplemented by DPA 2018 paragraph 4: Schedule 1.

Who we share 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.

De-identified and anonymous data obtained for the purposes of the Community Pharmacy Pilot is shared or is expected to be shared with:

- Cancer Alliances and local health delivery teams (including pharmacies) regularly throughout the pilot the purpose of service evaluation via aggregate management

information reports (with small number suppression where required) and to monitor progress and benchmark projects.

De-identified and anonymous data obtained under the Targeted Lung Health Check pilot is shared or is expected to be shared with :

- IPSOS UK - Aggregated datasets (with small number suppression where required) will be shared with to undertake the impact and economic evaluations to support the evaluation of the pilot.
- Cancer alliances and local Integrated Care Teams - Aggregated datasets (with small number suppression where required) will be made available for regions for ongoing monitoring and evaluation of their local services.

Other organisations may be able to apply to access the data we have collected, linked and analysed under the Cancer Programme Pilots Evaluation Directions following an application through NHS England's Data Access Request Service (DARS). Any data sharing will be subject to the organisations applying to access the data having a lawful basis to process it, and NHS England having a lawful basis to disclose it. 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. Where a DARS application is approved, data may be shared for analysis through the Data Access Request Service and NHS England Secure Data Environments, in line with NHS policy on Secure Data Environments

We may also publish anonymised data we have. This enables the NHS and other organisations to use this anonymous data for statistical analysis and for planning, commissioning and research purposes. We never publish any data that could identify you.

How long we keep data for

The minimum retention period for Cancer Programme Pilots data is 8 years after the closure of the Cancer Programme Pilots programme. This retention period will be reviewed regularly to ensure that the data is only held as long as is necessary our purposes in accordance with the NHS England Records Management Code of Practice 2021 and our Records Management Policy.

Where we store data

We securely store your data on our servers in the United Kingdom (UK).

Your data protection rights

Under data protection law, you have the following rights over your data for this collection:

- **Your right to be informed** – You have the right to be told how and why we are using your personal data. We have published this transparency notice to provide you with this information.
- **Your right to get copies of your data** – You have the right to ask us for copies of your personal data (right of access). For more information, see how to make a subject access request.
- **Your right to get your data corrected** – You have the right to ask us to correct (rectify) your personal data if you think it is inaccurate or incomplete.
- **Your right to limit how we use your data** – You have the right to ask us to limit the way we use your personal data (restrict processing) in certain circumstances.

To make request to exercise your data protection rights, email us at england.contactus@nhs.net

Opt-outs

National Data Opt-Out

When NHS England collects the Cancer Programme Pilots data from healthcare providers

If you have registered a National Data Opt-Out, NHS England can still collect your data under the Cancer Programme Pilots Directions 2024. This is because the National Data Opt-Out does not apply where NHS England has a legal obligation to collect the data (see section 6.4 of the National Data Opt-Out Operational Policy Guidance for more information).

When NHS England shares Cancer Pilots data

For any data we share with other organisations through our Data Access Request Service, we will apply the national data opt-out where it applies in line with the National Data Opt-Out Operational Policy Guidance.

You can find out more about and register a national data opt-out or change your choice on nhs.uk/your-nhs-data-matters.

Your right to complain

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

If you are not happy with our response, you 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 their website: ico.org.uk/make-a-complaint/

Changes to this notice

We may make changes to this notice. If we do, the 'last edited' date on this page will also change. Any changes to this notice will apply immediately from the date of any change.

NHS England » Those taking part in the Community Pharmacy Consultation Service for people attending Emergency and Urgent Care with a minor illness: NHS England is piloting a new service in Community Pharmacies to offer a consultation and cancer referral service for people who have attended urgent or emergency care with a minor illness or who need an urgent repeat prescription. This referral pathway from Community Pharmacies into secondary care is a crucial enabler for improving earlier diagnosis of cancer. The evaluation of the Pilot aims to aims to understand what works well, and less well and, if necessary, how it might be improved in the future.

Types of personal data we process – Community Pharmacy

We collect the following information from each of the Community Pharmacy Cancer Pilot sites:

Personal data, such as your

- NHS number
- Gender at birth
- Gender identity if different to that at birth
- Ethnicity
- Details of Community Pharmacy consultation
- Details of diagnoses following the Community Pharmacy referral

Targeted Lung Health Checks (NHS England » Evaluation of the Targeted Lung Health Check programme)

The targeted lung health checks programme is a new and ground-breaking flagship Pilot of work in England, offering free lung health checks to eligible people. This Pilot will contribute to the Cancer Ambitions of the NHS Long Term Plan, by improving the stage that Lung Cancers are being diagnosed and the survival for those diagnosed with Cancer. You can find out more about the TLHC service here: Lung health checks - NHS (www.nhs.uk)

Types of personal data we process – Targeted Lung Health Check

We collect the following information from each of the Targeted Lung Health Check Cancer Pilot sites:

Personal data, such as your

- Pseudonymised Patient Identifier
- Age
- Sex
- Ethnicity
- Details of any pre-existing health conditions
- Details of the Targeted Lung Health Check referral

Health Needs Assessment for Patients with Thalessimia

Purposes for processing

A Health Needs Assessment (HNA) has been commissioned by the NHS England, National Healthcare Inequalities Improvement Programme. Dr. Dianne Addei, (Senior Public Health Advisor) together with the Sickle Cell Disease & Thalassemia Healthcare Pathway Improvement Steering Group, will use the findings and recommendations of this HNA (due end November 2024) to inform and underpin service development and commissioning decisions.

The HNA will:

- Describe the cohort of Thalassemia patients – how many thalassemia patients there are in England, and their breakdown by age group, sex, ethnic group and deprivation level (Index of Multiple Deprivation).
- Understand the numbers of patients by type of thalassemia.
- Understand where these patients are being treated, including illustrating how many live close to specialist centres of care and how many are more distant.
- Understand aspects of their care such as how many emergency admissions they have had.
- Understand how many and what type of co-morbidities patients have.
- Understand their ages (in age bands) at diagnosis, and in relevant cases, ages at death.

Sources of the data

National Haemoglobinopathy Registry (NHR) and Secondary Use Services Data Collections (SUS) – Further information on the NHR can be found here - NHR – Home

Categories of personal data

Personal, Sensitive

Recipients of personal data

NHS England

Legal basis for processing

GDPR 6(1)(c), 6(1)(e) and 9(2)(h)

Types of Data Processed & categories of data

Personal Data
Personal Data which is:

- Directly Identifiable Data

will be processed for the purposes above about patients with Thalassemia.

Data that is processed by this Product may include about an individual's:

- name
- date of birth
- first part of post code
- gender
- NHS number and/or hospital record number
- health information, including information about your symptoms, medical conditions, diagnosis and, treatment

race or ethnicity

Legal grounds for processing personal data

Processing personal data

The processing of personal data by the NHS Trust using the NHR Registry for the purposes identified above is to provide individuals with care. This data is held within the National Haemoglobinopathy Registry.

This is permitted under the following legal grounds in UK GDPR:

UK GDPR

> **Public Task** - *Article 6(1)(e) '…necessary for the performance of a task carried out in the public interest or in the exercise of official authority…'.*

Confidential Data

The Personal Data processed for the purposes above is also Confidential Data.

As the NHS Trust are processing your Confidential Data to provide you with individual care, they are relying on your implied consent.

Who is Processing your Personal Data on behalf of the Controller

NHS England Arden and GEM CSU collect the data from the National Haemoglobinopathy Registry in order to de-identify it for analytical purposes.

Who your data is shared with

Other organisations
Personal data will not be shared with any other organisations
The Health Needs Assessment will not contain any personal data relating to individual patients. The outcome of the analysis will be shared with the Sickle Cell Disease & Thalassemia Healthcare Pathway Improvement Steering Group

Your rights under UKGDP

The following rights under UK GDPR apply to the processing of your Personal Data for the purposes above:

- Right to be informed
- Right of access
- Right to rectify
- Right to object

Other Opt Outs

The National Data Opt Out does not apply to the processing activities outlined as shown below:

- the collection, de-identification and analysis of data by NHS England to create the Health Needs Assessment has been carried out under a legal obligation (the Legal Directions) and therefore the National Data Opt Out does not apply in relation to this processing activity.
- the data to be shared with other organisations is no confidential patient information and therefore the National Data Opt Out does not apply.

If there is a separate request for data which falls outside of the above processing activities, the application of the National Data Opt Out will be assessed and applied where applicable.

Last updated Date

5th November 2024

Child Health Information Services Birth Notification Process for Unassisted births

Purposes for which the personal data is processed.

It is a legal requirement for a birth in England to be notified to a relevant body. The birth notification enables the necessary information about the birth, to be collected, processed and made available to health providers so that they can offer appropriate support to both mothers and babies.

Typically, midwives or doctors attending a birth will complete the notification, however, women have the legal right to give birth without a healthcare professional present; this is known as an unassisted birth.

Where no registered healthcare professional is present at the birth, the responsibility for the notification falls to the child's father (if present) or any other person attending the mother at the time of birth or within six hours afterward. This notification must be made within 36 hours of a birth to either NHS England (NHSE), an Integrated Care Board (ICB), or a Local Authority (LA).

NHSE has responsibility to commission the Child Health Information Services (CHIS) in England. These Services currently use a birth notification to create a CHIS record for the baby. Where an unassisted birth has taken place, it can be confusing for families to know how to complete the notification and who to send it to.

As a relevant body authorised to receive the birth notification because of an unassisted birth, NHSE have commissioned an existing CHIS provider to receive notifications on their behalf, from anywhere in England and to process them so that the relevant health services are informed about the birth.

South Central West Commissioning Support Unit (SCW CSU), operating as part of NHSE, will be the nominated CHIS and will therefore be processing the personal information contained in the birth notification as the relevant body and on behalf of NHSE.

Controller of the personal data

NHSE is the controller for the personal data being processed for the purposes of receiving, recording, and disseminating information reported through an unassisted birth notification.

Compliance with an Article 6 condition in the UK GDPR

The UKGDPR Article 6(1)(c) provides a lawful basis for processing where:

“Processing is necessary for compliance with a legal obligation to which the controller is subject.”

Birth notification is a legal requirement under Section 269 of the NHS Act 2006, National Health Service Act 2006 describes the requirements for reporting of births where no medical professional is present.

In addition, Article 6 (1) (e) provides a lawful basis for processing where 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. CHIS providers are commissioned by NHSE under the most up to date NHS public health functions agreement 2024 to 2025 - GOV.UK and therefore the nominated CHIS will be acting under this agreement on behalf of NHSE to exercise functions of the Secretary of State in sections 2A, 2B and 12 of the 2006 NHS Act to provide section 7A services. Where NHSE exercises these functions, they are referred to as ‘public health functions.’

In exercising the public health functions referred to above, NHSE must comply with the public sector equality duty (section 149 of the Equality Act 2010).

Types of personal data processed.

- Baby’s full name, or “Baby [Surname]” if a name has not yet been decided upon.
- Date and time of birth
- Address where the birth occurred.
- Mother’s address (if different to above)
- Name of the parent(s)
- Sex of the baby
- Name of any other person present with 6 hours of Birth.
- Email address of the person making the notification

How the personal data is obtained.

An unassisted birth notification is a self-declaration and will be sent to a dedicated e-mail address by the person making the notification. SCW CSU will receive this information.

How the personal data is processed.

SCW CSU will acknowledge the e-mail notification in the form of a ‘digital postcard’ which will be sent to the person who made the notification by e-mail. This will provide proof that the relevant body has been notified of the birth. The person who made the notification can then use that confirmation to have the birth registered by their Local Registrar of Births and Deaths.

SCW CSU will store the information received via the birth notification within their CHIS recording system which is called CarePlus Child Health and is provided by an organisation called SystemC.

The CHIS receiving the notification as the responsible CHIS provider for the child will create and maintain a record for that child in their own local recording system. This will either be

CarePlus Child Health or the SystmOne IT system provided by The Phoenix Partnership (TPP)

SCW CSU will not generate an NHS number when recording the birth notification following an unassisted birth.

Sharing the personal data

SCW CSU will share the birth notification with the CHIS that is responsible for that child either due to its address or registered GP. The receiving CHIS Provider will share the personal data with local health providers for the purposes of offering health care to the child where this is relevant. The local health providers include.

- GPs
- Newborn (neonatal) hearing screening providers
- Newborn blood spot providers
- Independent midwives
- Maternity departments
- Safeguarding teams
- Local authorities (children services)
- School-age vaccination providers
- School nurses
- Health visitor providers
- Other CHIS located outside the region (supporting children as they move around).

Where a relevant Data Sharing Agreement is in place, SCW CSU will also share the birth notification with the relevant ICB or LA as they are also relevant bodies for the purposes of the notification.

Under Section 436A of the Education Act 1996 each local authority has a legal obligation to:

- Be aware of children residing in its area.
- Investigate cases of children missing from education and ensure children not receiving statutory provision are receiving an adequate education.
- Undertake planning and development of services for children and young people

NHS England has a statutory responsibility under the Children Act 2004, Care Act 2014 and safeguarding provision within the Data Protection Act 2018 (Schedule 1, Part 2, Subsections 18 and 19) to ensure the safety of all children, and the safety of adults at risk of physical, mental or emotional harm and will share information to support this where this is appropriate.

How long the personal data is kept.

The CHIS service will retain your personal data for the period of time identified in accordance with the relevant – Records Management Code of Practice – NHS Transformation Directorate (england.nhs.uk) which will depend on the type of record the data is held in. This is likely to be until a child reaches the age of 25.

Other organisations with whom we share your personal data have obligations to keep it for no longer than is necessary for the purposes for which we have shared your personal data. Information about this will be in their transparency or privacy notices which are published on their websites.

Where the data is stored

We store and process the personal data within the United Kingdom but where our Processors need to process your personal data outside of the UK, we will always ensure that the transfer outside of the UK complies with data protection laws.

Unidentifiable statistical data may be processed outside of the UK.

Your rights over the personal data

To read more about the information we collect, our legal basis for collecting this information and what choices and rights you have, see – NHS England » NHS England as a data controller.

How to access the information held within a CHIS record

CHIS providers collect certain information from health and care organisations providing care to your child and would advise contacting your GP directly for a more complete record of their care or treatment.

If you would like a copy of the information held on the SCW CHIS in relation to an unassisted birth notification or have any queries or concerns about how SCW CHIS processes the notification, please send your request using the contact details below:

Address:

SCW CHIS Information Team
4th Floor, South Side,
Burlington House,
Crosby Road North,
Liverpool
L22 0QB

Telephone: 0300 561 1850

Email: **scwcsu.chis.administration@nhs.net**

SCW is a Commissioning Support Unit (CSU) hosted by NHS England.

The Data Protection Officer for NHS England is Jon Moore. The contact details for the office of the DPO are: england.dpo@nhs.net

Independent advice and complaints

For independent advice and complaints about data protection, privacy, and data-sharing issues, please contact:

Information Commissioner
Wycliffe House
Water Lane

Wilmslow
Cheshire SK9 5AF

Phone: 08456 306060 or 01625 545745 Website: **https://ico.org.uk/**.

Public and partners

How we use personal data when you contact us or work with us

People who contact our Customer Contact Centre

Purposes for processing

NHS England operates a customer contact centre which gives a central contact for members of the public, patients or their representatives to contact NHS England. This can be for individuals to register a complaint, request information (Freedom of Information, Subject Access), submit an enquiry or provide feedback.

Sources of the data

NHS England collects information when members of the public contact us. This can be when they ask a general enquiry through our contact centre or directly with teams. In doing so, we collect relevant information at the point of contact to resolve their enquiry.

Categories of personal data

The data collected by NHS England about the enquiry is primarily stored on our contact centre customer relationship management system. This includes a record for the individual with an associated file relating to their case (i.e. a general enquiry, freedom of information request, subject access request, access to medical records request, complaint etc.). Case files contain records of previous requests/contact types from that individual. They hold name, contact information and any other information relating to their case. There may also be instances where individuals contact specific teams in NHS England and information provided at this point will be collected (i.e. name and contact information).

Categories of recipients

The information is used by the contact centre and relevant teams to manage the response to the query within the organisation.

Subject access requests and access to medical records requests

- Primary Care Support England (PCSE) delivered by Capita Ltd manages responses to subject access requests and access to medical records requests for GP records. PCSE acts as a data processor for NHS England to manage GP health records for un-registered or deceased individuals.
- The Corporate Information Governance team manages responses to subject access requests and access to medical records requests for records held by NHS England other than GP records.

Freedom of Information and Environmental Information Regulations Requests

Information including personal data about the applicant is used by the Freedom of Information team to log and progress requests and for reporting purposes.

Information not including personal data about the applicant is used by:

- NHS England teams that hold any information relevant to the request.
- Capita under contract with NHS England in the handling of any relevant information that they hold on behalf of NHS England.
- Commissioning Support Units (CSUs) under contract with NHS England in the handling of any relevant information that they hold on behalf of NHS England.
- The NHSE Chief Executive Office and Media Team receive reports from the FOI team in-line with the monitoring of request types and trends.

Complaints

The information is used by the regional complaints teams to investigate and respond to the complaint.

Anonymous information from complaints may also be used by relevant teams within NHS England to learn from complaints to drive improvement to services and appropriately allocate resources.

Please see our contact centre webpage for more information.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'. For the processing of special categories (health) data the basis is 9(2)(h) – '…health or social care…'.

If your MP raises a matter with us on behalf of you

Purposes for processing

The Secretary of State for Health (SofS) is accountable to Parliament for the health system, including the business of NHS England. The Department of Health and Social Care (DHSC) supports the SofS in his role which includes accounting to Parliament for NHS England's performance and the effectiveness of the health and care system overall.

NHS England is an arm's length body of DHSC and shares responsibility for accounting to the public and to Parliament for policies, decisions and activities across the health and care sector. Accountability to Parliament will often be demonstrated through responses to parliamentary questions, MPs' letters, and appearances before parliamentary committees.

Categories of personal data

The data collected by NHS England is stored in the Parliamentary Business Team's central files. This will include a record for the individual with an associate file relating to their contact. Files may hold items such as individual's name, contact information and any other information relating to their communication. There may also be instances where individuals contact specific teams within NHS England. As such, information provided at this point will be collected (i.e. name and contact information).

Sources of the data

NHS England will collect information when members of the public, parliament or DHSC contact the organisation in relation to an MP request or Parliamentary Question. In doing so, NHS England collect relevant information at the point of contact to enable the team to provide a response to the request.

MP requests are often received by the NHS England Chief Executive Office and The National Medical Director's Office. They are then passed to the Parliamentary Business Team.

Categories of recipients

The information including information about the member of the public and MP is used by:

- Parliamentary Business Team
- NHS England Chief Executive Officer
- NHS England National Medical Director's Office

- Any other team within NHSE that may directly receive such requests

The request information not including personal data about the applicant is used by:

- NHS England teams that hold any information relevant to the request.
- Capita under contract with NHS England in the handling of any relevant information that they hold on behalf of NHS England.
- Commissioning Support Units (CSUs) under contract with NHS England in the handling of any relevant information that they hold on behalf of NHS England.

Legal Basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For the processing of special categories data, the basis is Article 9(2)(h) '…health or social care…'.

If you get involved in our work as a 'Patient and Public Voice (PPV) Partner'

Purposes for processing

Patient and public participation is an essential part of NHS England's way of working. We want to build strong and supportive relationships with our Patient and Public Voice (PPV) partners, so that we can work in partnership and use people's experiences and views to inform our work. The term PPV Partners includes patients, service users, carers and families, and the general public.

Our approach to working with our PPV Partners is set out in our PPV Partner Policy, which describes four different types or categories of PPV Partner role:

- PPV partners who choose to attend, respond or comment on open access engagement opportunities e.g. responding to online surveys or attending a meeting in public
- PPV partners who are invited to attend workshops/events/ focus groups on a one-off basis
- PPV partners who are a member of a working group which meets regularly
- PPV partners who are in senior PPV roles that demonstrate strategic and accountable leadership and decision making activity.

Sources of the data

The data is provided by PPV Partners when registering to attend a meeting or event, and / or when applying to a specific PPV Partner role (through submitting an application form).

Categories of personal data and recipients

The information provided on the application form includes:

- name
- age address and postcode
- e-mail address
- whether the applicant can access e-mail
- whether the applicant is a
    - patient or health service user (current or previously)
    - carer of a patient currently / previously using health services
    - Representative of a patient organisation
    - Other
- Ability to use telephone, e-mail, and internet to communicate and take part in meetings
- Ability to commit time
- Other PPV roles
- Skills and experience
- Any access or support needs to enable participation
- References

The information is used to identify and engage with PPV Partners, and enable communication and involvement in PPV activities..

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'.

Subscribers to our mailing lists

Purposes for processing

NHS England will in the routine course of its business need to communicate with stakeholders across the business (i.e. with all Clinical Commissioning Group (CCG) Accountable Officers, all Commissioning Support Units or for certain programs and initiatives. These communications are either to provide relevant stakeholders important information in relation to their business or that of NHS England. Other communications may be in relation to a project to which interested parties have subscribed for further information

as and when it is available (i.e. event attendance, updates on project progress or canvassing feedback on documentation for initiatives).

Categories of personal data

Name and contact (email) information.

Sources of the data

Contact information is primarily collected by teams in the routine course of their work with relevant stakeholders, i.e. it is deemed appropriate a mailing list is created to canvass responses or feedback on documentation. It may also be collected on request, i.e. colleagues or members of the public contact NHS England and ask to be placed on a relevant mailing list for updates.

Categories of recipients

The information is used by NHS England, its hosted bodies, or data processors acting on our behalf.

Legal Basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'.

Social prescribing

Purposes for processing

Social prescribing involves helping patients to improve their health, wellbeing and social welfare by connecting them to community services which might be run by the council or a local charity. For example, signposting people who have been diagnosed with dementia to local dementia support groups.

The NHSE Social Prescribing team is currently supporting NHS, Health Providers and the Voluntary Community and Social Enterprise (VCSE) with social prescribing development. The contact lists are used to contact social prescribing contacts who have requested to be part of the social prescribing regional networks so that network members can keep up-to-date with social prescribing development and to also share information and good practice. Details held within the contact lists are provided by the attendees of the Social Prescribing

team events and as such, the information is supplied to the Social Prescribing team voluntarily.

Categories of personal data

The contact lists contain the following information categories:

- Full Name
- Job Title
- Location
- Workplace
- Telephone number – mobile
- Email address

Sources of the data

The data is provided by Social Prescribing members/stakeholders.

Categories of recipients

The information is used by the Social Prescribing team to contact the relevant Social Prescribing contacts.

Legal Basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'.

Clinical Pharmacists in General Practice

Purposes for processing

NHS England's Clinical Pharmacists in General Practice programme supports the introduction clinical pharmacists working in GP practices. This is part of a wider expansion of the general practice workforce so that patients have better local access to a range of highly trained health professionals for their needs. NHS England is responsible for approving applications for the scheme. We commission a research organisation to evaluate the programme and training and development providers. We commission the procurement of training and development providers and will commission a research organisation to evaluate the programme.

To apply for the scheme a lead contact submits an application form via the Clinical Pharmacists Portal. The lead contact acts on behalf of the practice(s) for the application. He or she is the contact for queries with the application, to send information about the programme, and is a point of contact for training and development providers.

We communicate directly with clinical pharmacists to provide information about the programme. We provide their contact details to the organisation that will be undertaking an evaluation of the programme, to ensure that they can be involved in the evaluation. We also use information about them to ensure that only the people we fund as part of this programme have access to the training and development that NHS England commissions.

Sources of the data

Lead contacts or someone working on their behalf submit information about themselves via the Clinical Pharmacists Portal.

Quarterly reports are submitted by or for the practices in which the clinical pharmacist is working, with their details. The Clinical Pharmacist may enter their own details, or it could be another person in the practice or a person in another organisation that forms part of the bid.

Categories of personal data and recipients

About the Lead Contact: name and email address.

About the Clinical Pharmacists: name, e-mail address and General Pharmaceutical Council number.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'.

Those completing surveys or questionnaires

Purposes for processing

NHS England uses a range of different surveys as a valuable source of feedback directly from patients, services users and NHS staff about the care that they receive or provide. The surveys that we conduct annually involving the processing of personal data are described below. For other surveys, please refer to the privacy notice provided with the survey.

GP Patient Survey

The GP Patient Survey assesses patients' experience of general practice services , including experience of access to GP practices, the quality of care received from healthcare professionals and experience of NHS urgent care services. The survey also includes a number of questions assessing patients' experience of NHS dental and pharmacy services. The GP Patient Survey is currently conducted by Ipsos who act as a data processor on behalf of NHS England.

Sources and categories of personal data

The mailing list for the GP Patient survey is produced from the registered GP patient list that is held by NHS England. A random probability selection of patients (aged 16+) is selected from all eligible GP practices, and the names and addresses, and where available, mobile phone numbers and emails of the selected patients are sent to Ipsos who distributes the questionnaire on our behalf. Once the survey is finished Ipsos destroys the contact details that it has received. Unless patients have consented to be contacted again for future research.

Each survey response has a unique reference number. Ipsos uses this survey number to (i) identify who has responded to the survey (so they only send reminders to people who haven't responded), (ii) to link responses to GP practices, and (iii) to weight the responses by linking to the age and gender of respondents. The survey responses are never linked to the patients' personal details, unless patients have consented to have their contact details linked to their survey responses in order to be contacted again for future research.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For special categories (health) data the basis is Article 9(2)(h) '…health or social care…'.

Subjects' rights

If someone does not want to receive reminders about this survey, they may send back a blank questionnaire or contact Ipsos on a Freephone number provided with the questionnaire. They may also inform Ipsos that they wish to permanently opt out of the survey.

Categories of recipients

The individual answers to the survey are combined with the answers from other people who have responded so the data can be analysed by approved NHS England staff. They are not linked to names, NHS numbers or health information. Approved researchers may be granted access to the data for specified uses via an application process.

Aggregated data are published at national, ICS, PCN and GP practice levels. Small cell counts are suppressed in the published data so that individuals cannot be identified from their responses.

Retention period

All name and address information is destroyed within six months of the end of the survey fieldwork period, unless patients have consented to be contacted again for future research.

National Cancer Patient Experience Survey

The National Cancer Patient Experience Survey is currently conducted by Picker Institute Europe who act as a data processor on behalf of NHS England. The aim of the survey is to provide insight on patient experience of cancer care and treatment. It has been designed to monitor national progress as well as to provide information to drive local quality improvements.

Categories of personal data

The data we use for administering the survey includes names and addresses, sex, ethnic group, date of birth, diagnosis code, admission and discharge dates, trust code, site treated at, specialty code, referring ICBs, admission type, and NHS number.Where available the patients email address and mobile phone number are also collected. We need the diagnosis code to verify the patients' diagnosis of cancer.

Sources of the data

Patients (aged 16+) who received cancer care as an inpatient or day case and were discharged in particular months of the survey year receive the questionnaire. Patient details are obtained from the NHS Trusts who have provided the care.

Categories of recipients

NHS England uses the survey data to carry out further analysis by linking the data to the National Disease Registration Service database. . For this further analysis, we will use the survey data with your NHS number, postcode and date of birth, but not name or full address. Approved researchers receive anonymised data under license from NHS England.

Retention period

The name, address, date of birth, NHS number and the last part of the patient's postcode is used to identify patients to take part in the survey. This will be destroyed within 12 months, after publication, unless patients have consented to be contacted again for future surveys.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For special categories (health) data the basis is Article 9(2)(h) '…health or social care…'.

NHS England and Picker Institute Europe have obtained section 251 approval (of the NHS Act 2006 and Health Service (Control of Patient Information) Regulations 2002). This provides a legal basis for patient information to be used to carry out the survey. Patients consent to the use of the information they provide in the questionnaire.

This survey has been granted exemption from the National Data Guardian opt-out by the Department of Health and Social Care. For more information see: National Data Opt-Out - NHS England Digital

Subjects' rights

Patients can opt out of receiving the questionnaire by informing the Trust that has treated them The Trust provides information on how to do this. Patients can also withdraw the information given in the survey upon request, up to the point at which data are analysed and personal details removed. A helpline number is given on the survey materials.

Under 16 Cancer Patient Experience Survey

The Under 16 Cancer Patient Experience Survey is currently conducted by Picker Institute Europe who act as a data processor on behalf of NHS England. The purpose of the survey is to collect patient experience feedback from children and young people with cancer. The aim of the survey is to provide insight and gain a better understanding of children and young

people cancer patient experience. The survey has been designed to monitor national progress as well as to provide information to drive local quality improvements.

Categories of personal data

The data we use for administering the survey includes names and addresses, sex, ethnic group, date of birth, diagnosis code, discharge dates, site treated at, speciality code, admission type, and NHS number.

Sources of the data

Patients (aged under 16) who received cancer care or treatment as an inpatient or day case and have been discharged within a recent twelve month period. Patients must have a confirmed primary diagnosis of cancer or a non-malignant brain, other central nervous system or intracranial tumour. Patient details are obtained from the NHS Trusts who have provided the care.

Categories of recipients

NHS England uses the survey data to carry out further analysis by linking the data to the National Cancer Registration and Analysis Service. The recipients do not receive names and addresses but do need NHS Numbers for linkage purposes. Approved researchers receive anonymised data under license from NHS England.

Retention period

The name and address information relating to this survey will be destroyed within twelve months of publication of the survey results, unless an erasure request is made sooner.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For special categories (health) data the basis is Article 9(2)(h) '…health or social care…'.

NHS England and Picker Institute Europe have obtained section 251 approval (of the NHS Act 2006 and Health Service (Control of Patient Information) Regulations 2002). This provides a legal basis for patient information to be used to carry out the survey. Patients consent to the use of the information they provide in the questionnaire.

This survey has been granted exemption from the National Data Guardian opt-out by the Department of Health and Social Care. For more information see: National Data Opt-Out - NHS England Digital

Subjects' rights

Patients or their parents can opt out of receiving the questionnaire by informing the Trust that has treated them. The Trust provides information on how to do this. Patients or their parents can also withdraw the information given in the questionnaire upon request, up to the point at which data are analysed and personal details removed. A helpline number is given on the questionnaire.

NHS Staff Survey

The purpose of the NHS Staff Survey is to collect staff views and experiences of working in the NHS and to provide information for deriving national and local performance indicators relating to staff engagement, diversity and inclusion. The survey is carried out on behalf of trusts and other NHS organisations by third party survey contractors who contract directly with the trust. The contractors submit the data to the NHS Staff Survey Co-ordination Centre who are the national data processor for NHS England and provide benchmarking reports for each organisation along with national reports. The data is used to improve local working conditions for staff, and ultimately to improve patient care.

NHS England can make data from the NHS Staff Survey available to researchers. The team share anonymised datasets (where individuals cannot be identified) as well as case level pseudonymised data where there are no direct identifiers.

Access is granted through a formal Data Sharing Agreement (DSA) process, which ensures any use of data complies with legal, ethical, and data protection standards. Researchers must clearly outline their intended use, demonstrate a valid research purpose, and commit to safeguarding the confidentiality of NHS staff. All research use must align with the principles of responsible data handling and contribute to the broader understanding of NHS workforce experiences.

Sources and categories of personal data

Information is provided by employing organisations from the entries in the Electronic Staff Record for their employees. This includes name, work address, and/or e-mail address. It also includes full name, age, directorate, department or division, location, job title and staff group, maternity, pay band; ethnicity; long-standing illness, health problem or disability.

These variables help verify the representativeness of the staff list, where a sample is being used. Disability/pay band data were requested for the first time in 2017 following requests for this data from the WDES team to monitor equality. Collecting this information allows the monitoring of non-response rates by ethnicity/occupational group.

Categories of recipients

The responses to the survey are collated by the survey contractors and the response data are sent to the Staff Survey Co-ordination Centre. The Co-ordination Centre is then able to provide organisations with data to compare their performance with other organisations of a similar type and also produce national statistics for NHS England. The responses to the survey remain confidential. Completed questionnaires are submitted directly to the independent survey Contractor. The employing organisation does not have access to the completed questionnaires or to any linked personal data (e.g. names and addresses). The report that is sent back to the organisation presents the survey findings in summary form, and does not reveal the identity of the staff sampled. To help preserve anonymity, the Co-ordination Centre will not provide feedback on any group from which there are 10 or fewer responses.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'. For the processing of special categories (health) data the basis is Article 9(2)(h) – '…health or social care…'.

International Survey of Health Experience (ISHE)

Purposes for processing

The International Survey of Health Experience (ISHE) is otherwise known as the Patient-Reported Indicator Surveys (PaRIS) and is an initiative of the Organisation for Economic Cooperation and Development (OECD). Countries are working together to develop, standardise and implement a new generation of indicators that measure the outcomes and experiences of health care that matter most to people.

ISHE will assess the outcomes and experiences of patients with long-term conditions managed in primary care across countries. The survey aims to fill a critical gap in primary health care, by asking primary care providers (in England that will be GP practices) and patients about aspects like access to health care and waiting times, as well as quality of life, pain, physical functioningnd a psychological well-being.

Sources of the data

The mailing list for the ISHE is produced from the registered GP patient list that is held by NHS Digital. A random probability selection of patients (aged 16+) is selected from all eligible GP practices, and the names and addresses of the selected patients are sent to Ipsos who distributes the questionnaire on our behalf. Once the survey is finished Ipsos destroys the contact details that it has received.

Each survey response has a unique reference number. Ipsos uses this survey number to (i) identify who has responded to the survey (so they only send reminder letters to people who haven't responded), (ii) to link responses to GP practices, (iii) to weight the responses by linking to the age and gender of respondents. The survey responses are never linked to the patients' personal details.

Categories of personal data and recipients

The data we use for administering the survey includes names and addresses, sex, NHS number, GP Practice code, phone number (if available), partial date of birth and sex.

Legal basis for processing

For UK GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'.

National Diabetes Experience Survey

Purposes for processing

The National Diabetes Experience Survey is currently conducted by Ipsos who act as a data processor on behalf of NHS England. The aim of the survey is to provide insight on experiences of care and self-management for people living with diabetes. It has been designed to provide national insight and data for Integrated Care Systems (ICS) to support a person-centred policy to delivering care for people living with diabetes.

Sources of the data

The sample is drawn from the National Diabetes Audit (NDA), a list of people who are living with diabetes. This list was matched with the Personal Demographic Service (PDS) database, a list of patients registered with a GP, to obtain contact details.

Categories of personal data

People are eligible for the survey if they are recorded as living with type 1 or type 2 diabetes in the NDA, aged 18 or over, diagnosed at least 12 months ago, and living in England.

The data we use to select people to take part in the survey includes sex, age band, ethnicity, type of diabetes, date of diagnosis, care processes/clinical outcomes, treatment targets, treatment type, GP practice code, Lower Layer Super Output Area (LSOA), and NHS number. The data we use for those invited to take part in the survey includes name, address, mobile number (where available), and month and year of birth.

Each survey response has a unique reference number. Ipsos uses this survey number to (i) identify who has responded to the survey (so they only send reminder letters to people who haven't responded), (ii) to link responses to Integrated Care Systems (ICS), and (iii) to weight the responses by linking to the age and gender of respondents. The survey responses are never linked to the patients' personal details.

Recipients of personal data

The individual answers to the survey are combined with the answers from other people who have responded so the data can be analysed by approved NHS England staff. AGEM DSCRO will use the survey data to carry out further analysis by linking the data to the National Diabetes Audit and other healthcare databases. AGEM DSCRO will not receive the name or address of any individuals, but will require NHS number for linkage purposes. Approved researchers may be granted access to the data for specified uses via an application process.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For special categories (health) data the basis is Article 9(2)(h) '…health or social care…'.

NHS England and Ipsos have obtained section 251 approval (of the NHS Act 2006 and Health Service (Control of Patient Information) Regulations 2002). This provides a legal basis for patient information to be used to carry out the survey. Patients consent to the use of the information they provide in the questionnaire.

The Department of Health and Social Care has confirmed that this survey has been made exempt from the National Data Opt Out. The list of exemptions and policy postponements

provides more information: Programmes to which the National Data Opt-Out should not be applied - NHS England Digital

Subjects' rights

An analytical team within NHS England (AGEM DSCRO) are responsible for sharing the NDA and PDS data with Ipsos. People living with diabetes can opt-out of their data being shared with Ipsos, before sampling takes place, by contacting AGEM DSCRO. Information on how to do this will be advertised by NHS England before sampling takes place.

If someone has been invited to take part and does not want to receive reminders about this survey, they can contact Ipsos on a Freephone number provided in the invitation letter. They may also inform Ipsos that they wish to permanently opt out of the survey.

Patients can also withdraw the information given in the questionnaire upon request, up to the point at which data are analysed and personal details removed.

Retention period

All name and address information is destroyed by Ipsos after 2 months of publication of the survey, unless an erasure request is made sooner.

Integrated Care Experience Survey (ICES)

Purposes for processing

The ICE Survey is currently conducted by Ipsos who act as a data processor on behalf of NHS England. The aim of the survey is to provide insight on experiences of care and to help understand the extent to which integrated care is working from a service user and their unpaid carers' perspective. It has been designed to provide national insight and data for Integrated Care Boards (ICB) to understand where joined-up care is working well and where experience of care can be improved.

Sources of the data

The sample will be identified though GP records (via the data processor for each ICB) based on the eFI score. This a score that is derived from a measure of frailty based on the accumulation of a range of 36 deficits.

Categories of personal data

The survey will initially target service users with clinically complex needs identified though GP records (via the data processor for each participating ICB) based on their eFI score as this is seen as a cohort with complex clinical health and care needs and likely to be in contact with multiple health and care providers.

People are eligible for the survey if they are recorded as aged 18+ and have moderate or severe frailty score. The data items set out below are required for each of the ICB data processors to identify the cohort and draw the survey sample:

NHS number, Title, Full name, Address, Postcode, Mobile number, Date of birth, Gender, Ethnic category, GP Practice code, Data sharing flag, Registrations status, Registration date, Code type, Clinical Code, Clinical Term.

Initial invitees will be provided with a letter to pass to their carer, if they have one, with informal carers then also having the opportunity to provide feedback through a separate informal carers' questionnaire.

Each survey response has a unique reference number. Ipsos uses this survey number to (i) identify who has responded to the survey (so they only send reminder letters to people who haven't responded), (ii) to link responses to Integrated Care Systems (ICS), and (iii) to weight the responses by linking to the age and gender of respondents. The survey responses are never linked to the patients' personal details.

Recipients of personal data

Once the survey fieldwork has finished, the programme will be using the data to recontact people (where the survey respondent has consented for this to happen) for future iterations of the survey. The following data items will used for that purpose:

Full name, address, email, mobile number.

Once the survey fieldwork has finished, the programme will be using the survey dataset to link the responses to other datasets (where the survey respondent has consented for this to happen). Along with survey responses, the following data items will be used for that purpose:

NHS number, date of birth, postcode.

Legal basis for processing

For UK GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For special categories (health) data the basis is Article 9(2)(h) '…health or social care…'.

NHS England and Ipsos have obtained section 251 approval (of the NHS Act 2006 and Health Service (Control of Patient Information) Regulations 2002). This provides a legal basis for patient information to be used to carry out the survey. Patients consent to the use of the information they provide in the questionnaire.

The Department of Health and Social Care has confirmed that this survey has been made exempt from the National Data Opt-Out. The list of exemptions and policy postponements provides more information: Programmes to which the National Data Opt-Out should not be applied - NHS England Digital

Clinical Networks and Senate

Purposes for processing and categories of personal data

Strategic Clinical Networks (SCN) bring together those who use, provide and commission the service to make improvements in outcomes for complex patient pathways using an integrated, whole system approach. SCN serve in key areas of major health and wellbeing challenge, currently:

- cardiovascular (including cardiac, stroke, renal and diabetes)
- maternity, children and young people
- mental health, dementia and neurological conditions
- cancer

Clinical Senates have been established to be a source of independent, strategic advice and guidance to commissioners and other stakeholders to assist them to make the best decisions about healthcare for the populations they represent.

The personal data we process include:

- name and contact details of patients, healthcare colleagues and other stakeholders
- personal data contained in expressions of interest for positions within the Networks and Senate, CVs, information arising from the interview process, and pen-picture biographies
- personal data relating to claims for expenses

Sources of the data

- Patients, healthcare colleagues and other stakeholders
- Healthcare providers

Categories of recipients

The data are used by the Clinical Networks and Senate Teams in NHS England.

Legal basis for processing

For the GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'.

Clinical Entrepreneur

Purposes for processing and categories of personal data

As part of the NHS Mandate, NHS England has developed the Clinical Entrepreneur Training Programme which is designed to offer opportunities for junior doctors and wider health professionals to develop their entrepreneurial aspirations during their clinical training period. The Clinical Entrepreneur Training Programme forms part of NHS England's wider programme of innovation.

NHS England process the following categories of personal data in relation to the Clinical Entrepreneur Training Programme:

- Name and contact details
- Date of birth
- Educational and employment background
- Any other information provided within individual CVs
- Information relating to their innovation proposal and progress in its development

The purposes for processing the above categories of personal data are:

- To ensure the suitability of individuals applying for the programme
- To ensure the suitability of the mentoring and educational events available to applicants
- To maintain distribution lists in relation to the programme
- To maintain distribution list in relation to other events and funding opportunities

Sources of the data

The data is provided by applicants, partners and mentors to the programme

Categories of recipients

- University and higher education training partners
- Department of Health and ALBs
- Other Government Departments
- Academic Health Science Networks (AHSNs)
- Heath charities, third sector organisations and social enterprises
- Health industry organisations
- Mentors to the programme (selected by applicants to the programme)

Legal basis for processing

For the GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'.

National Innovation Accelerator

Purposes for processing and categories of personal data

National Innovation Accelerator is hosted by UCL Partners although we commission/contribute financially to the programme. For applications to the programme they use the fluid review system which is accessed by UCL Partners for assessment purposes; within our team we can also access all data should we wish as follows:

- name and contact details
- professional registration number
- personal data supplied in application made to the programme, such as biographical details/place of work/organisational details
- references
- letters of support
- personal data contained in shortlists or processed as a result of interviews
- personal data comprised in press releases or other publicity materials (such as case studies)
- a personal sprint plan

Categories of recipients

Recipients of the data include:

- The Research and Innovation team
- The Innovation team

- Academic Health Science Networks
- Assessors (NHS England, NHS Digital, Partner Organisations, external experts)
- Partner organisations
- The media and the public

Legal basis for processing

For the GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'.

Counter fraud

Purposes for processing

NHS England has a team of Accredited Counter Fraud Specialists with responsibility for the prevention and detection of fraud, bribery and corruption against the organisation. When allegations are made suggesting that NHS England has been the victim of an economic crime, the Counter Fraud Team will conduct an investigation. This may involve; gathering evidence, obtaining witness statements and interviewing suspects. If evidence of a crime is found, the suspect may face disciplinary proceedings, (including referral to professional body), civil sanctions, and/or criminal proceedings.

We work closely with the NHS Counter Fraud Authority, who has oversight of cases as they progress and in the case of prosecutions, act as a gateway for initial file submissions to the Crown Prosecution Service.

Perpetrators of economic crime against NHS England can be anyone associated with the Health Service, including:

- patients,
- employees,
- primary care contractors, (GPs, dentists, opticians, pharmacists)
- suppliers.

In order to establish if a criminal offence has occurred, NHS England may request access to personal data. Primary care contractors are obliged under regulations to provide information to NHS England that is reasonably required in connection with their contract, such as counter fraud activities. Service Condition 24 of the NHS Standard Contract requires providers to allow Counter Fraud Specialists access to information that is relevant to the detection and investigation of cases of bribery, fraud or corruption.

Categories of personal data

In order to carry out our activities to prevent and detect economic crime we may process the following data:

- Contact details such as names, addresses, telephone numbers
- Emergency contact(s)
- Education and training, incl. development reviews (appraisals)
- Patient data, incl. GP, dental optical and pharmaceutical records
- Offences (including alleged offences), criminal proceedings, outcomes and sentences
- Employment details, (employment contract, salary, position etc.)
- Information around travel and subsistence; expenses
- Employment / identity records (including professional membership, qualifications, references and proof of identity and eligibility to work in the UK)
- Bank details
- Pay, benefits and Pension details (incl. National Insurance number)

Please note this list is not exhaustive and may change over time.

Categories of recipients

Details of cases are entered on to the National Counter Fraud Authority's case management system.

The NHS England Counter Fraud Team may also work alongside Clinical Commissioning Groups and NHS Business Services Authority in the investigation and prevention of fraud, bribery and corruption.

When a case is submitted for prosecution, information including personal data is sent to the Crown Prosecution Service.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…task carried out in the public interest or in the exercise of official authority…'. This applies to investigation by NHS England, and co-operation with the NHS Counter Fraud Authority, Clinical Commissioning Groups and NHS Business Services Authority.

For the processing of special categories data the basis is 9(2)(g) – '…substantial public interest…'. This is supported by Schedule 1 Part 2 paragraph 10 (preventing or detecting unlawful acts) and paragraph 14 (preventing fraud) of the Data Protection Act 2018.

The National Fraud Initiative

NHS England is required to protect the public funds it administers. It may share information provided to it with other bodies responsible for; auditing, or administering public funds, or where undertaking a public function, in order to prevent and detect fraud.

The Cabinet Office is responsible for carrying out data matching exercises.

Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

We participate in the Cabinet Office's National Fraud Initiative: a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to the Minister for the Cabinet Office for matching for each exercise.

The use of data by the Cabinet Office in a data matching exercise is carried out with statutory authority under Part 6 of the Local Audit and Accountability Act 2014.

Data matching by the Cabinet Office is subject to a Code of Practice. Should you wish to know more information on this Fair Processing Notice please see the more detailed full text. View further information on the Cabinet Office's legal powers and the reasons why it matches particular information. For further information on data matching at this authority contact Stuart Francis at stuart.francis@nhs.net.

Legal basis for processing

For the GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…', or where there is a legal obligation to share information Article 6(1)(c) – processing is necessary for compliance with a legal obligation to which the controller is subject.

If you Speak Up to NHS England

Purposes for processing

Speaking Up is the term used when a worker contacts us with a concern about an organisation and its services. The concern will typically (although not necessarily) be

regarding something they have witnessed at work. Full details can be found here: Whistleblowing: guidance for prescribed persons - GOV.UK (www.gov.uk)

NHS England is a “prescribed person” (i.e. an organisation responsible for handling cases of Speaking Up under the Public Interest Disclosure Act 1998) and can investigate cases relating to Primary Care Organisations (i.e. General Practice; Local Dentistry; Opticians; and Community Pharmacy Services).

NHS England also operates its own internal policy for concerns raised by its staff. This can be found here: NHS England » NHS England external freedom to speak up policy for NHS workers

Further details available on NHS England’s website and dedicated Speaking Up contact pages.

Categories of personal data

Data collected can be anonymous from the person Speaking Up depending on the nature in which the information is provided. Other times, name, contact details and specific elements relating to the concerns may be collected, i.e. personal information regarding another employee , or those concerned to be at risk (name, contact information etc.) .

Sources of the data

Information will be provided by the person Speaking Up regarding themselves and those involved in the issues leading to the concerns raised, or those considered at risk.

Categories of recipients

The information is used by:

- NHS England and relevant teams for the purposes of investigation
- With the person Speaking Up’s consent, we can refer the issue to an alternative external body such as the following:
  - Fraud and corruption – NHS Counter Fraud Authority
  - Serious patient safety issues or issues relating to condition of registration – Care Quality Commission
  - Allegations regarding a clinician’s fitness to practice – relevant professional regulator or healthcare body (CQC)
  - Where local resolution has not been possible – NHS England

- Offender Health – details of prescribed persons for Police and Justice Services can be found on the Whistleblowing Prescribed Persons Pages.
- The National Offender Management Service has its own Reporting Wrongdoing Hotline, which is 01527 544777
- Safeguarding- Issues will be dealt with in accordance with NHS England safeguarding policies.

Legal basis for processing

For the GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For the processing of special categories data the basis is Article 9(2)(h) '…health or social care…'.

People Pulse Project

Purposes for processing

The aim of the *"People Pulse"* project is to support active listening and understanding of the views of NHS employee experiences which will help shape actions at a local, regional and national level.

Sources of data

This project is not mandatory and those NHS employees who wish to participate are able to provide their information which will be collected and administered via a website www.nhspeoplepulse.com/england.

Categories of personal data and recipients

The data voluntarily provided will be: NHS organisation, region, job type, gender, ethnicity, disability, age, sexual orientation and carer arrangements. This data is necessary for synthesising information for our decision making on what further support we can provide to the provider organisations.

Legal basis for processing

For GDPR purposes NHS England's

lawful basis for processing is: *Article 6(1)(e) – '…exercise of official authority…'* and for processing special categories (health) data the bases are: *Article 9(2)(b) – '…support NHS employees…' and 9(2)(h) – '…for health or social care…'.*

NHS Innovation Service

Purposes for processing and categories of personal data

The NHS Innovation Service acts as an 'information gateway' to support people developing new innovative products, services or initiatives in healthcare ('innovators'), to understand processes such as the regulations and standards they will need to meet, the real-world evidence they will need to demonstrate, and NHS procurement and reimbursement processes. It will act as a single entry point for innovators to register for support and/or to apply for certain programmes.

Organisations providing support to innovators are able to communicate directly both with the innovator and with each other to help the innovator compile a single record of their progress and evidence generated to date.

The categories of personal data processed are:

- Name
- Contact details
- Job title
- Organisation

Categories of recipients

Please check the NHS Innovation Services webpage for published partners and up to date categories of recipients: innovation.nhs.uk/about-the-service/who-we-are

International Data Processing

To support the delivery of the NHS Innovation Service, some personal data may be securely processed by one of our contracted service providers based in Portugal, which is subject to relevant adequacy regulations under section 17A of the Data Protection Act 2018.

Legal basis for processing

For the UKGDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'.

Retention period

Your data will be stored for a period of six years in accordance with NHS England's corporate retention schedule.

Annual Health Checks Focus Group

NHS England are working together with the National Children's Bureau as a data processor on a project for an Annual Health Checks (AHC) Focus Group, an initiative to explore the views of children and young people aged 14-19 years with a learning disability, and to support them to co-design communications and materials to improve the quality of these services and make them more accessible. NHS England is responsible as a data controller for the processing of personal data for the purposes of the AHC Focus Group project.

Purposes for processing

We collect personal data from children and young people and their families or carers to participate in the AHC focus group through the sharing of thoughts and experiences of AHC to highlight key themes and points raised.

Participants who agree to take in part will have their discussions recorded for a video resource on AHC, which will be shared with NHS health professionals across all the NHS for training purposes, which includes sharing on NHS websites, and anonymised quotations through NHS social media channels.

Categories of personal data

The following types of personal data are processed:

- Application form: name, contact details, date of birth, participation access needs.
- Equality and Diversity monitoring: disability, health impairments, ethnicity, religion. This data is collected separately to application to ensure anonymity.
- Video: Within the above activities we will be recording the focus group to be used in a video resource for NHS healthcare professionals, we will therefore be collecting

personal data regarding your experiences in video format. NHS England will use the video for:

- Training: shared with NHS health professionals across all the NHS for training purposes
- Social media: including, Facebook, Twitter, Instagram and YouTube (anonymised quotes only)
- NHS England website

National Children's Bureau will be collecting quotes during these activities. These quotes will not be identifiable to individuals and will be used by National Children's Bureau and NHS England for 5 years in the following ways:

- Used in the project report National Children's Bureau submits to NHS England for this project
- Used in promotional materials, bids and other reports, training, and on social media by National Children's Bureau and NHS England

Legal basis for processing

For UKGDPR purposes NHS England have a lawful basis of Article 6(1)(a) Consent for the processing of application forms and videos for the purposes of the AHC review. NHS England has a further lawful basis of Article 6(1)(e) – '…exercise of official authority…' arising from a statutory duty to secure continuous improvement in the quality of service and to promote education and training (of health and care staff), which will apply to the processing of the videos for NHS staff training purposes and reporting purposes.

NHS England have a lawful basis for processing special category personal data under UKGDPR Article 9(2)(a), explicit consent.

Data recipients

Your personal data is received and used by:

- NHS England (video and reporting)
- National Children's Bureau (application, video and reporting)
- Other voluntary sector organisations such as Mencap, National Development Team for Inclusion and Contact (video)

Retention period

Your data will be stored for a period of six years following project end in accordance with NHS England's corporate retention schedule.

NHS 111

Purposes for processing

When you call NHS 111 from a mobile phone, mast data are used to route your call to a local NHS provider. These data can locate the device to a small geographic area (typically, within 100m of the device). A local NHS provider is often best placed to deal with your call. Where you are using WiFi calling or we are otherwise unable to determine your location, we will ask you whether we may seek your consent to use geolocation data to route your call to a local NHS provider. These data provide GPS co-ordinates for the device (which can be accurate to a small number of metres). Where you do not wish to provide consent, your call will be picked up and you will be asked for the name of the nearest large town or city. This information is captured by Natural Language Processing, and used to route your call to a local NHS provider. Any mast and geolocation data are stored separately, not shared with any recipient, and deleted after 24 hours.

Categories of personal data

- calling line identification data (CLI data)
- mast data (where available)
- geolocation data (where there is consent)

Categories of recipients

- Vodafone Group Plc provides the telephony service for NHS 111 under contract to NHS England

Legal basis for processing

For GDPR purposes, NHS England's lawful basis for processing is Article 6(1)(e) – '…task carried out in the public interest or in the exercise of official authority…'.

For the processing of special category (health) data, the condition is Article 9(2)(h) – '…health or social care…'.

For the use of geolocation data (only), consent is a requirement of The Privacy and Electronic Communications (EC Directive) Regulations 2003.

Cancer Vaccine Launch pad

Purposes for processing

The NHS Cancer Vaccine Launch pad (CVLP) is a project that acts as a bridge to enable NHS patients with cancer to participate at the earliest possible opportunity in cancer vaccine trials and to accelerate the development of cancer vaccines.

The aim of the CVLP is to provide a basis for accelerated development of personalised cancer vaccine treatment, by providing a standardised, high quality, expanded standard of care pathway for tumour molecular analysis and sequencing incorporating elements of the NHS Genomic Medicine Service.

The primary objective is to identify and recruit cancer patients who might be suitable for personalised cancer vaccine trials.

Sources of the data

Members of the direct care team at local NHS Hospital Trusts will collect patients' personal information as part of routine care. In most cases, consultants or cancer specialists will identify patients who might be eligible for cancer vaccine and connect them with a research nurse who will then provide more detailed information.

Categories of personal data

- Patient personal data and contact details
- Patient clinical record
- Patient blood and tissue sample

Categories of recipients

- Data Controllers: NHS England, CVLP participating NHS Hospital Trusts and colorectal cancer research trial sites.
- Data Processors are Cellular Pathology Genomics Centres (CPGC).

Legal basis for processing

- Art 6.1e Public authority

- Art.9.2a Explicit consent
- Art.9.2h Health or social care system
- Art.9.2i Public health

Graduate Management Training Scheme

Purposes for processing

The NHS Graduate Management Training Scheme (GMTS) provides fast-track leadership development for trainees across six different specialisms.

Trainees are employed on a fixed-term contract throughout their time on GMTS; they are employed by NHS Business Services Authority (BSA) on behalf of NHS England, and NHS England manage the scheme. All employment processes for trainees are managed by NHS BSA, in conjunction with NHS England, including: contracts, payroll, policies and procedures.

Each Trainee is placed with one or more NHS organisations (or organisations providing NHS-funded services) during their time on the Scheme.

Trainees undertake post-graduate qualifications with one of a number of education providers depending on their specialism.

The duration of the scheme is two years to two and a half years. Data will be retained in line with NHS England's Records Retention Policy.

Sources of the data

Data is provided by users on application and employment to the Scheme. Additional information is collected from individuals on initial logon to our trainee management system and ongoing administration of management and progression through the Scheme.

Categories of personal data

The NHS Graduate Management Training Scheme and associated contractors outlined below process different categories of personal information. NHS England process personal demographics, education and training data and medical information in order to administer the GMTS.

Categories of recipients

Additional recipients of data are:

- NHS Business Services Authority – process personal data for the purpose of employment of the trainee.
- GMTS recruitment team and contractors supporting recruitment process (Amberjack) - For the purpose of recruitment
  Education providers

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'. For the processing of special categories data the basis is Article 9(2)(h) – '…health or social care…'.

NHS England as a Data Controller

NHS England is the data controller for the personal data processed for the management of the GMTS.

NHS BSA is the data controller for personal data processed for the employment of those placed on the GMTS.

For information in regard to NHS England's Data Protection Officer, how to enact a subject's rights request and for lodging a complaint with the Information Commissioner about any aspect of the processing of the personal data please visit: NHS England » NHS England as a data controller

Talent Management Programme

NHS England's Privacy Notice describes how we use your personal data and explains how you can contact us and exercise your rights as a data subject.

Purposes for processing

NHS England collects personal data about you to understand the talent within NHS boards and sub-boards. This data will be used to send individuals information about training, development opportunities, and evaluations related to appraisals.

Any information related to Equality, Diversity, and Inclusion (ED&I) will be used to assess the diversity of internal talent and to offer targeted training and development. Providing ED&I data is optional.

Personal data is collected from the point of creating an account to access the system and during relevant Leadership and Management activity.

Categories of personal data

- Name
- Email address
- Region
- Sector
- Organisation
- Profession
- Job Title
- Age
- Gender
- Ethnicity
- Disability (as defined by the Equality Act 2010)

Categories of recipients

We ensure that personal data is accessed and used only by staff who need it to support Leadership and Management activities, or as required by law. Data may also be shared with partner organisations under data sharing agreements, but only for Leadership and Management purposes. For reporting, all personally identifiable data will be anonymised. Your identifiable diversity data will not be shared outside of the NHSE Talent & Leadership team without your consent.

Legal basis for processing

- where NHS England process personal data about you, we use Article 6(1)(e) of the UK GDPR: exercise of official authority.

- where NHS England process special categories of personal data about you, including any revealing racial or ethnic origin, we use Article 9(2)(h) of the UK GDPR: Health or social care (with a basis in law) The basis in law is Equality Act 2010, Section 149.

Safety and Quality

How we use personal data for safety and quality purposes

Incidents

Purposes for processing

NHS England is committed to the improvement of quality and delivery of services and uses incident events, investigation, evidence and reports relating to incidents under various policy and procedural structures.

An incident requiring investigation is defined as an incident that occurred in relation to NHS-funded services and care resulting in unexpected or avoidable death, harm or injury to patient, carer, staff or visitor. In order to promote quality and compliance, NHS England has several reporting protocols for incidents and provides investigation and learning to improve systems and services across the organisation.

Sources of the data

Incident events are recorded across the organisation, and within systems and services commissioned by NHS England. Under various protocols including Serious Incidents Requiring Investigation (SIRI), Never Events, Deaths In Custody, Neonatal Death, these incidents will be investigated and reviewed with a view to ensuring improvement in outturn and performance.

Categories of personal data

The data received by NHS England includes a record for each incident including (if relevant) patient or staff name, NHS Number and other personal details, including relevant healthcare records and information about the incident, including others involved or impacted by the event.

Categories of recipients

The information is used by the relevant team or department together with Nursing and Quality, and Improving Health and Quality teams in NHS England. Anonymised “lessons learned” will be cascaded to relevant parties within (or outside) NHS England to ensure that improvements are delivered.

Please see our Serious Incident Framework Policy web page and National Reporting and Learning System framework for more information.

Legal basis for processing

For the GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For the processing of special categories data the basis is Article 9(2)(h) '…health or social care…'.

Care and treatment reviews

Purposes for processing and categories of personal data

Care and Treatment Reviews (CTRs) are part of NHS England's commitment to transforming services for people with learning disabilities, autism or both. They are used by commissioners for people living in the community and in learning disability and mental health hospitals. They are helping to reduce the number of people going into these hospitals.

CTRs also help to improve the quality of care people receive in hospital by asking key questions and making recommendations that lead to improvements in safety, care and treatment. They reduce the amount of time people spend in hospital and bring people together to help to sort out any problems which can keep people in hospital longer than necessary. They do this by helping to improve current and future care planning, including plans for leaving hospital. Further information can be found here.

NHS England processes personal data to organise CTRs. The personal data NHS England processes include:

- Name and home address
- NHS number
- date of current admission and estimated date of discharge
- your consent to the Care and Treatment Review
- date(s) and venue(s) of panel meeting(s)

NHS England processes the above categories of personal data for the following purposes:

- Management and organisation of the CTRs
- For repatriation purposes of patients

Sources of the data

- Patients
- Providers of health care

Categories of recipients

Providers of health care (including the CTR panel members consisting of experts by experience)

Legal basis for processing

For the GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For the processing of special categories data the basis is Article 9(2)(h) '…health or social care…'.

Controlled drugs accountable officer – alerts etc.

Purposes for processing

Role of the Controlled Drugs Accountable Officer

Regional Lead Controlled Drugs Accountable Officers (CDAOs) are responsible for all aspects of Controlled Drugs management. The roles and responsibilities of CDAO's are governed by the Controlled Drugs (Supervision of Management and Use) Regulations 2013.

All organisations within the region are required to report controlled drug incidents and concerns to the CDAO. The Lead CDAOs are required to set up Controlled Drugs Local Intelligence Networks (CD LINs) to share concerns and good practice within their area. Whilst we can determine the specific membership, it is largely comprised of the CDAOs across the area, Clinical Commissioning Group representatives and the relevant regulators and agencies as set out in the regulations.

Cascade Alerts – sharing personal and sensitive information

Incidents of significant concern locally e.g. patients or healthcare professionals fraudulently obtaining Controlled Drugs, prescriptions, patient alerts would need to be shared through a cascade alert with healthcare professionals including GP Practices, Dental Practices, Hospitals, Community Pharmacies and other relevant healthcare providers. These alerts may contain sensitive personal information to help prevent further fraudulent activity and prevent harm to the public.

Personal sensitive information shared on alerts is usually provided to us by the police and other healthcare professionals who request us to send out an alert on a local standard NHS England Template with the NHS Logo. We facilitate this process and on some occasions this information may only be alleged concerns.

Private Prescriber Applications

The lead CDAO also receive requests from healthcare professionals to be able to order stock of CDs via requisitions and / or prescribe Controlled Drugs Privately and accordingly manage these applications with a lot of personal information included.

Sharing and reporting Fitness to Practice Concerns and Criminal Activity

Where the lead CDAO has concerns about a healthcare professional's fitness to practise they will share this information with the professional regulator and or other relevant bodies across the NHS. Information on criminal activity would be shared with the police and counter fraud agencies

Sources of the data

We receive information / unproven intelligence from:

- Members of public
- Registered healthcare professionals
- Non-registered healthcare staff
- NHS and Private Healthcare organisations/providers
- Counter Fraud Agencies
- Commissioners
- Police CDLOs
- Regulators
- NHS England Colleagues
- Voluntary organisations
- Anonymous

Categories of personal data

CDAOs would very rarely send out an alert with any sensitive information.

- Full Name
- Personal Address
- Organisation Address
- Date of Birth
- Email addresses
- NHS Number
- Photographs
- Professional Registration Number
- Description of alleged claim(s)

Categories of recipients

We may share information and intelligence to relevant organisations:

- GP Practices
- Dental Practices
- NHS and Private Hospitals
- Community Pharmacies
- Other healthcare providers
- Voluntary Organisations
- Police
- Counter Fraud Agencies
- Commissioners
- Regulators
- NHS England Colleagues
- Other CDAOs
- CDAOs and relevant departments outside of England Footprint e.g. Scotland, Wales, Northern Ireland
- NHS Business Services Authority
- Primary Care Services England
- Local Authorities
- Public Health Departments
- Indemnity Insurance Providers
- Adult and children safeguarding boards

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For the processing of special categories (health) data the basis is Article 9(2)(h) '…health or social care…'.

Safety alerts

Purposes for processing

NHS England is committed to the delivery of safe and efficient services, and will communicate safety critical information and guidance to the NHS under various policy and procedural structures.

An Alert may be issued to prevent or avoid unexpected or avoidable death, harm or injury to patient, carer, staff or visitor, or in order to prevent fraud.

Sources of the data

Alerts can be generated across the organisation, and instigated from systems and services commissioned by NHS England. Under numerous protocols including regulations for Controlled Drugs, Patient Safety, Medical Devices etc., and these alerts will be cascaded to relevant parts of the NHS to ensure patient safety and protection.

Categories of personal data

The data received by NHS England includes a record for each Alert including (if relevant) patient or staff name, NHS Number and other personal details, including relevant healthcare records and information about the Alert, including others involved or potentially impacted by the Alert.

Categories of recipients

Alerts can be cascaded throughout the NHS, and are directed, on a necessary and proportionate bases, to any relevant team within (or outside) NHS England. When Alerts are sent to relevant people they may include action to be taken, or raise awareness of potential harm to which staff need to be aware.

Please see the MHRA CAS Pages for details and NHS England Alerting Systems framework for more information.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For the processing of special categories data the basis is Article 9(2)(h) '…health or social care…'.

Safeguarding

Purposes for processing

NHS England is dedicated in ensuring that the principles and duties of safeguarding adults and children are holistically, consistently and conscientiously applied with the wellbeing of all, at the heart of what we do.

Categories of personal data

The data collected by NHS England staff including its hosted bodies in the event of a safeguarding situation will be as much personal information as is necessary or possible to

obtain in order to handle the situation. This is likely to be special category information (such as health information).

Sources of the data

NHS England will either receive or collect information when someone contacts the organisation with safeguarding concerns or we believe there may be safeguarding concerns.

Categories of recipients

The information is used by:

- NHS England staff including its hosted bodies when handling a safeguarding incident.
- NHS England may share information accordingly to ensure duty of care and investigation as required with other partners such as Local Authorities, the Police, healthcare professional (i.e. their GP or mental health team).

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For the processing of special categories data, the basis is Article 9(2)(b) – 'processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law…'

Assuring Transformation

Purposes for processing

NHS England uses Assuring Transformation Data to check that people with a learning disability, autism or both are getting the right care in the right place. Please see our Assuring transformation data web page and What is assuring transformation for more information about how we do this.

NHS Digital publishes a monthly progress report. This lets the public check if the NHS is doing a good job of looking after people with a learning disability, autism or both who are in hospital. The progress reports don't have any personal information, like names, birthdays or NHS numbers.

Sources of the data

Commissioners of health services (the people who plan and pay for services) collect the data in the first place from the hospitals that are treating these patients. The commissioners are NHS England, Lead Providers in Provider Collaboratives acting on behalf or NHS England and Clinical Commissioning Groups across the country. Every month NHS Digital collects the information from the commissioners and gives it to NHS England, who is responsible for the collection.

Categories of personal data

The data received by NHS England includes a record for each patient with their name, NHS Number and other personal details, and information about their stay in hospital.

Categories of recipients

The information is used by the Learning Disability Programme within NHS England to derive performance and quality indicators for Learning Disability services, in order to drive improvements in the services and to identify where good/poor practice is taking place.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is 6(1)(e) '…exercise of official authority…'. For special categories (health) data the basis is 9(2)(h) '…health or social care…'.

NHS England has obtained section 251 support (approval under the Health Service (Control of Patient Information) Regulations 2002) to collect Assuring Transformation data from providers of specialised mental health services, and to receive the Assuring Transformation Dataset from NHS Digital.

If you are a patient assigned to the Special Allocation Scheme

Purposes for processing

It is important that practices can maintain a safe environment for their patients and all staff working in the practice. NHS Regulations allow a GP practice to immediately remove a patient from their list following any incident where a GP or member of practice staff has feared for their safety or wellbeing, resulting in the incident being reported to the police.

Special Allocation Schemes were created to ensure that patients who have been removed from a practice patient list can continue to access healthcare services at an alternative, specific GP practice. NHS England has a responsibility to ensure that all patients can access good quality GP services and that patients are not refused healthcare following incidents that are reported to the police.

Patients are registered on the scheme by the submission of a Violence Reporting Form to NHS England, or CCG with Delegated Authority by a GP practice. Patients are sent a letter informing them that they have been registered on the scheme.

Sources of the data

The data are provided on the Violence Reporting Form submitted by a GP practice. Authorised signatories on the form are GP Partner, Practice Manager or Deputy Practice Manager.

Categories of personal data

The data included on the Violence Reporting Form includes:

- Name
- Date of birth
- Address
- NHS No
- Details of the incident
- Actions taken by police
- Whether the patient has an existing mental health condition, with details
- Medical Conditions, particularly where these may have an effect on the patients' behaviour. E.g. Their Mental Health Status, any learning disabilities, Drug or Alcohol abuse
- Existing medications
- Please provide the contact details of any other Health Care providers, e.g. Mental Health Team Workers, District Nurses, or Health Visitors and confirm that you will inform them that the patient will be placed on the Violent Patient Scheme subject to approval of the referral request

Categories of recipients

Primary Care Support England process the forms submitted by GP practices.

Legal Basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For the processing of special categories (health) data the basis is Article 9(2)(h) '…health or social care…'.

Health care professionals

How we use personal data about health professionals that we have responsibility for

Performers Lists

Purposes for processing

The National Health Service (Performers Lists) (England) Regulations 2013 (Performer List Regulations) as amended provides the regulatory framework for managing medical, dental and ophthalmic performers who perform primary care services and entrusts the responsibility for managing the performers lists to NHS England as the commissioner of primary care services. NHS England's Framework for Managing Performer Concerns sets out NHS England's governance arrangements for operationalising the Regulations.

NHS England has statutory responsibility for managing the England Performers Lists for GPs, General Dental Practitioners and ophthalmic practitioners who undertake NHS primary care services under the respective primary care contracts. The Performers Lists provide assurance to prospective employers that the performer is suitable and eligible to undertake services and for this reason is included as part of the suite of pre-employment checks undertaken. NHS England is required by statute to make the Performers List available to members of the public and this provides them with the assurance that the primary care practitioner is safe and fit to practise.

For further information please refer to NHS England's performer list policies and procedures.

Sources of the data

Applications for inclusion must be made by sending NHS England an application in writing in line with Regulation 4 of The National Health Service (Performers Lists) (England) Regulations 2013 as amended.

Categories of personal data

The personal data includes; full name, sex, date of birth, residential address and telephone number. For further information please refer to the National Performers List Application Form.

Categories of recipients

Primary Care Support England (PCSE) is responsible for administering entry and status changes to Performer Lists on behalf of NHS England.

Legal basis for processing

For the GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For the processing of special categories data, the basis is Article 9(2)(h) '…health or social care…'.

Managing performance concerns

Purposes for processing

The National Health Service (Performers Lists) (England) Regulations 2013 (Performer List Regulations) as amended provides the regulatory framework for managing medical, dental and ophthalmic performers who perform primary care services and entrusts the responsibility for managing the performers lists to NHS England as the commissioner of primary care services. NHS England's Framework for Managing Performer Concerns sets out NHS England's governance arrangements for operationalising the Regulations.

To meet our obligations we have established a framework for managing performer concerns. This framework encompasses:

- the process for considering applications and decision making for inclusion, inclusion with conditions and refusals to be undertaken by NHS England's local offices;
- the process by which teams identify, manage and support primary care performers where concerns arise; and
- the application of NHS England's powers to manage suspension, imposition of conditions and removal from the performers lists.

NHS England has established Performance Advisory Groups (PAGs) and Performers Lists Decision Panels (PLDPs) within local teams in order to support its responsibility in managing the performance of primary care performers. The PAG's role is to consider concerns about a named individual, who is either included on the Performers List, has a prescribed connection to NHS England, or is a Pharmacist, and determine the most appropriate course of action. It can instruct an investigation where it considers it appropriate and it can agree voluntary undertakings with a performer when low level concerns have been identified and the performer accepts this to be the case. The primary role of the PLDP is to make decisions under the Performers Lists Regulations. This does not prevent the PLDP from taking any action that the PAG can take.

Sources of the data

The data sources are far-reaching and data may be provided by anyone raising a concern with regards to primary care practitioners.

Categories of personal data

The data includes the identity of the performer, details of the concern and the details of the person raising the concern as well the outcomes of any action taken regulatory or not.

Categories of recipients

The data is received by performance advisory groups and performers list decision panels. Records are held by teams in NHS England's Medical Directorate and Commissioning Operations Directorate. Regulatory or law enforcement bodies may be informed as deemed necessary.

Legal basis for processing

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For the processing of special categories data the basis is 9(2)(h) '…health or social care…'.

Medical revalidation

Purposes for processing

Medical revalidation is a process for evaluating that a doctor is up to date and fit to practise, introduced in December 2012. Every licensed doctor who practises medicine in the UK must have an annual appraisal and recommended as being up to date and fit to practise, by their responsible officer to the GMC, every five years. All designated bodies with connected doctors must appoint a responsible officer to oversee the revalidation of their doctors.

The (national) Senior Level Responsible Officer (SLRO) for Medical Revalidation in NHS England, supported by the four (regional) Higher Level Responsible Officers (HLRO), must be assured that all responsible officers and designated bodies are discharging their statutory responsibilities and will support them to achieve this. The SLRO in NHS England is also responsible for the revalidation of primary care medical practitioners in England that are on the medical performers list.

In order to allow NHS England to discharge its duties as a designated body, the personal details of all doctors in England, appraisers and responsible officers, (together with the contact details of administrators, Medical Directors, Clinical Appraisal Leads and Chief Executives of designated bodies in England), are held within NHS England's Revalidation Management System (RMS). The system links to GMC Connect to make revalidation recommendations and also to ensure that the databases remain synchronized.

The medical revalidation and appraisal processes have been designed so that the appraisal inputs are confidential between the doctor and their appraiser. For more information about the use of information during the revalidation please refer to the Medical Appraisal Documentation Access Statement. Also the Medical appraisal policy – Annex H regarding Information Governance.

To facilitate payment of appraisals, RMS holds the supplier reference number for the appraisers and in some cases it also holds information such as the National Insurance Number and Pension Scheme Reference number where NHS England manages the pension contributions.

Sources of the data

The data is obtained from the appraisees, appraisers and responsible officers in designated organisations.

Categories of personal data

The RMS system includes personal details of doctors who have been appraised. It also includes information on education and employment history, alleged criminal offences and convictions, and health information, where relevant, to their appraisal. To facilitate payment of appraisers, RMS holds the supplier reference number for the appraisers and in some cases it also holds information such as the National Insurance Number and Pension Scheme Reference number where NHS England manages the pension contributions.

Categories of recipients

The information in RMS will primarily be accessible to responsible officers and their administrative staff. However, certain other persons, including medical directors and regulatory bodies, may have access to the information, as explained in the access statement, referred to above. The information in RMS will only be shared with other organisations for the purposes of medical revalidation or otherwise where there is a legal power to do so, with the agreement of NHS England's Caldicott Guardian.

Legal basis for processing

For the GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For the processing of special categories data, the basis is Article 9(2)(h) '…health or social care…'.

Midwives – Local Supervisory Authority

Purposes for processing and categories of personal data

NHS England holds archive records relating to Local Supervising Authorities. Those records concern the eligibility to practise of midwives and information captured to support the safety and quality of maternity care. The information was largely held in a database that has been migrated to NHS England's system and there are also some holdings in hard copy.

The personal data we process include:

- name and contact details
- professional registration number
- a personal development plan and an annual appraisal
- action plans
- any personal data in records relating to serious incidents or Fitness to Practise investigations and outcomes

Sources of the data

- Midwives
- Providers of health care

Categories of recipients

- The Nursing team in NHS England
- Nursing and Midwifery Council
- Providers of health care

Legal basis for processing

For the GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'. For the processing of special categories data the basis is 9(2)(h) '…health or social care…'.

General Practice Pay Transparency

Purposes for processing

Pay transparency in general practice was introduced into the GP Contract Regulations in October 2021. The Department of Health and Social Care (DHSC) subsequently confirmed that the implementation of general practice pay transparency was to be delayed. The data collection has now been resumed beginning with 2021/22 NHS earnings.

On 1 October 2022, amendments to the NHS (General Medical Services Contracts) Regulations 2015 (the 'GMS Regulations') and the NHS (Personal Medical Services Agreements) Regulations 2015 (the 'PMS Regulations') came into effect to require certain other individuals, namely 'job holders', to self-declare their NHS earnings if these are above the earnings threshold for the relevant financial year. These changes are also reflected in an amendment to The Alternative Provider Medical Services (APMS) Directions 2022. GMS, PMS and APMS contracts have been varied to incorporate these amendments.

Categories of personal data

Individuals who are in scope are required to confirm their name and job title and to declare the following information:

- their NHS earnings for the relevant year
- the organisation(s) from which the NHS earnings were drawn.

Further information, including on the definition of NHS earnings for the purpose general practice pay transparency, is included in the general practice pay transparency guidance.

Sources of the data

The following individuals will be required to make a self-declaration on an annual basis if their NHS earnings exceed the threshold for the relevant year:

- individuals who hold the GP contract as partners (including partners who are not GPs) and contractors who are individual medical practitioners
- partners of clinical sub-contractors and sub-contractors who are an individual (including partners of any onward clinical sub-contractors and any onward clinical sub-contractor who is an individual)
- individuals who work for (are engaged by) either a contractor (regardless of whether the contractor is an individual medical practitioner, a partnership or a limited company) or clinical sub-contractor (including any onward clinical sub-contractors) under either:
    - a contract of employment

    - a contract for services
    - or as a company officer (directors and any company secretary)
- Individuals engaged by a third party to provide clinical services (for example a locum engaged via an employment agency).

The thresholds of NHS earnings for the financial years 2021-22 to 2023-24 above which a self-declaration must be made are set out below:

- 2021-22 - £156,000
- 2022-23 - £159,000
- 2023-24 - £163,000.

Categories of recipients

The information self-declared is intended for publication in a national publication to include for each individual and the relevant year:

- name
- job title
- their NHS earnings in £5,000 earnings bands
- the names of the organisations from which they drew NHS earnings from in the relevant year.

Legal basis for processing

The Secretary of State for Health has provided NHS England with direction to carry out this activity.

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'. For the processing of special categories data the basis is Article 9(2)(h) – '…health or social care…'.

Return to Practice Programme

Purposes for processing:

The Return to Practice Programme will support eligible returners to undertake their self-directed return to the Health and Care professions council register.

Support and funding in the form of a stipend is available to the following:

HCPC Returners

- All former HCPC registrants who live in England and plan to return to work in England once returned to the Health and Care Professions Council (HCPC) register.

- Those who have gained a UK HCPC approved programme more than 5 years ago and have never been registered and never practised.

- Registrants who remained on the HCPC register for more than two years but have not practised and consider themselves to be out of practice.

Nurse and Midwife Returners

NHS England (NHSE) is committed to support former nurses and midwives returning to practice who undertake a return to practice programme / Test of Competence (ToC), self-funding the process and reside in England.

Returners may be eligible for reimbursement of test fees, travel and accommodation—provided specific conditions are met.

Sources of data:

All personal data processed will be provided by those who are eligible to NHS England.

Categories of personal data and recipients:

Personal data processed by NHS England will include name, contact details and bank account details (in order to receive a stipend or reimbursement). NHS England will not share the data with any other party.

Legal Basis for processing:

For GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) '…exercise of official authority…'.

Our workforce

How we use personal data for employment purposes

Purposes for processing

We process your personal data in the main because the processing is necessary for the purposes of a contract of employment we have with you. In some cases, we may process

information only once we have received your consent for us to do so. In other cases, we will process data in order to comply with legal requirements, both contractually and non-contractually. The reasons for which we may process your personal data may include (but are not limited to):

- Staff administration (including payroll)
- Pensions administration
- Workforce planning, and provision of facilities such as estates, car parking and IT
- Equal Opportunities Monitoring
- Staff health and wellbeing, safety and security, e.g. CCTV and staff identity badges
- Provision of Management Information
- Surveying of staff to support organisational initiatives
- Business management and planning
- Accounting and Auditing
- Accounts and records
- Crime prevention, detection of fraud and prosecution of offenders
- Education
- Management of organisational change
- Supporting emergency preparedness and business continuity
- Health administration and services
- Compliance with obligations, e.g. returns to Cabinet Office / Government departments

Categories of personal data

To carry out our activities and obligations as an employer / engaging body we may process the following data:

- Contact details such as names, addresses, telephone numbers
- Emergency contact(s)
- Education and training, incl. development reviews (appraisals)
- Employment / identity records (including professional membership, qualifications, references and proof of identity and eligibility to work in the UK)
- Bank details
- Pay, benefits and Pension details (incl. National Insurance number)
- Information around travel and subsistence; expenses
- For staff driving a vehicle for work purposes: vehicle details, details of driving licence and vehicle insurance, tax, MOT etc.
- Personal demographics (including protected characteristics such as gender, race, ethnicity, sexual orientation, religion, date of birth, marital status, nationality)
- Medical information including mental and physical health
- Information relating to health and safety
- Trade union membership
- Offences (including alleged offences), criminal proceedings, outcomes and sentences

- Employment Tribunal applications, Employee Relations cases, complaints, accidents, and incident details
- Employment details (position details, salary, full time equivalent (FTE) etc., status in relation to organisational change)
- Support provided under employee assistance programmes

Please note this list is not exhaustive and may change over time.

Information sharing and recipients

There are a number of reasons why we may have to share your personal information with third parties.

There may be circumstances where information is shared without your consent, for example:

- The disclosure is necessary for a statutory function of NHS England or the third party to whom the information is being disclosed
- There is a statutory obligation to share the data; for example, making returns to the Cabinet Office, Department of Health, Office of National Statistics etc.
- Disclosure is required for the performance of a contract
- Disclosure is necessary to protect your vital interest; for example in medical emergency situations
- Disclosure is made to assist with prevention or detection of crime, or the apprehension or prosecution of offenders
- Disclosure is required by a Court Order
- Disclosure is necessary to assist NHS England to obtain legal advice

We may need to share your information with the following organisations/categories of organisations (further detail below):

- Other employers - to obtain pre-employment references or to enable you to undertake a secondment or corporately sponsored volunteer role
- Disclosure and Barring Service (DBS) - obtain employment background checks and necessary criminal record checks
- Occupational health provider - information about your health and attendance to enable them to provide advice and guidance to HR and your manager.
- Payroll and pensions providers – to process your pay and pension

- Employee benefits providers - to allow them to support you with the employee benefits services you wish to take up
- ICT providers – to grant you access to ICT systems necessary to perform your role
- Training and development providers – to enable you to undertake approved learning and development activities
- Survey providers - to collect views from our staff and report on staff engagement within the organisation
- Publications – NHS England publishes information about certain staff, including their name and job titles. This information can be found here: https://www.england.nhs.uk/contact-us/pub-scheme/what-we-do/

Specific information about recipients of personal data and the data shared can be found below.

Department of Health and Social Care (DHSC)

NHS England will share data with DHSC data relating to its organisational structure namely: names of senior individuals (salary Band 9 and above), individual job titles, grade, directorate and sub-directorate.

The purpose of this is for:

- Understanding the numbers of staff working in different areas and assurance that resources are being prioritised in line with ministerial priorities
- Understanding the make-up of staffing in order to help shift resources flexibly and quickly when major events or new priorities emerge (e.g. Covid, Brexit)
- Analysing where there are teams undertaking similar functions across different parts of the system (DHSC and individual ALBs) with a view to identifying opportunities for efficiencies.

The 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 Controllers.

The Personal Data to be shared under this Agreement will assist the Secretary of State in the discharge of their duties relating to the promotion and provision of the health service in England (including public health functions), as outlined in Part 1 of the NHS Act 2006 (as amended by the Health and Social Care Act 2012).

Recruitment, Employee Records and Contracts Administration (NHS Business Services Authority)

NHS England are working to establish integrated Human Resources services, and the components of this joint service will be designed and implemented during 2019/2020. The purposes related to employment for which we currently process personal data jointly are:

- Staff recruitment
- Equal opportunities monitoring
- Line management

Staff recruitment

NHS England has established a joint recruitment service, and are responsible as a controller for the processing of personal data that you provide on your application, and from other sources. We have engaged the NHS Business Services Authority (NHSBSA) to process applications for employment on our behalf.

NHS BSA works with NHS England through each stage of the recruitment process using our end-to-end recruitment system TRAC, this includes pre- and post-interview activities up to confirming the offer of employment and issuing a contract. If you applied for a vacancy using NHS Jobs your application will be imported into the TRAC recruitment system and all information you receive about your application will be generated by TRAC. You may be invited to create a TRAC account if you are shortlisted to enable your application to be managed through the system.

We will use information you have provided to verify your identity when we speak to you, and at all stages of the application process.

For successful applicants

Before agreeing a contract, we will use the information you have provided to complete the following pre-employment checks in line with NHS Employers' guidance:

- Professional registration checks
- Employment history and reference checks
- Disclosure and Barring Service (DBS) check (if required)
- Work health assessment: to check you are fit to work or confirm what reasonable adjustments are required, if applicable
- Confirming Right to Work, identity, and eligibility for the vacancy
- Meeting safeguarding law requirements where this is relevant to the vacancy role

NHS England are also required to monitor the diversity of candidates to ensure we comply with the Equality Act 2010.

Categories of recipients

We share your information with:

- medical professionals, to assess your fitness to work and any reasonable adjustments that you need
- the Disclosure and Barring Service (DBS), if your role requires a DBS check
- with named referees to obtain a reference
- any other organisation who has a legal right to it.

Your information will not be transferred outside the European Economic Area (EEA),

Keeping your personal information

For non- successful applications, personal information in the e-recruitment system will be deleted within 400 days of the advertised application closing date. This information is retained so that we can revisit vacancies and applications in case the vacancy needs re-advertising or to enable us to respond to any candidate queries.

Successful applications will remain in the system for 400 days, but only information relevant to the employment of successful candidates will be retained within staff employment records. This will be specified in your contract of employment. If you withdraw at offer stage, you will not receive any further information and your details may still be retained for 400 days securely outside of the e-recruitment system.

Equal opportunities monitoring

We have established a joint analytics team that is responsible for analysing data to enable reporting on compliance with equal opportunities requirements by NHS England. This supports workstreams such as the Workforce Race Equality Standard, the public sector Equality Duty and the Gender Pay Gap, which are mandatory for NHS employers.

Record level staff data is required to enable analysis by data items representing any characteristics relevant to equalities monitoring. Personal data including employee number is obtained from the Electronic Staff Record and other sources for example appointments to roles.

The dataset extracted includes employee number, data about role including grade and pay scale, position, type of contract, working hours, also protected characteristics including gender, ethnic origin, disability, marital status, sexual orientation, age band, religious belief.

The employee number is required to enable linkage between datasets.

Access to personal data including employee number is restricted to members of the joint analytics team.

Line management

Managers have access to the Electronic Staff Records of their staff and use this to keep employment details up-to-date and manage the development of their staff, training compliance, annual leave and other absence. Managers use personal data relating to the health of their staff for the following purposes:

- Reimbursement of expenses
- Maintenance of professional registration
- Sickness absence management
- Maternity and adoption
- Occupational Health and accommodating special workplace needs.

Sickness absence management

As an employer, NHS England have legal duties to ensure the health and safety of their employees at work, and that their employees receive their sickness pay allowance entitlement. We must also ensure that we comply with employment rights legislation around sickness absence.

Managers need to know that that their staff are fit for work and be aware of adjustments that may be to necessary to support staff following a period of sickness. For these purposes they will receive GP fit notes from the staff that they manage. These indicate whether or not an individual is fit for work and may give advice on any support required to accommodate an illness or condition when returning to work.

Managers will also receive return to work forms completed by their staff, and conduct return to work interviews to agree on any adjustments required.

Managers must ensure that the Electronic Staff Record (ESR) for their staff is kept up to date with sickness absence records. This enables us to comply with employment rights legislation when managing sickness absence.

By analysing the data extracted from the ESR we are able to identify and address any inequalities and target health and wellbeing interventions.

Maternity, paternity and adoption

Managers are responsible for ensuring that the rights of their staff are respected when they are to become mothers or fathers.

They will receive completed MATB1 and matching certificates, which confirm details around a pregnancy or adoption. These forms are shared with HR and payroll ensuring communication with the employee about their entitlements and correct payment during periods of leave.

Occupational Health and accommodating special workplace needs

Line managers may refer a member of staff, with their consent, for an occupational health assessment.

The NHS England Occupational Health Providers are external providers. Managers will share your contact details and referral with the providers as required.

Managers will receive occupational health reports to inform them of any adjustments that are required.

Workforce Race Equality Standard

The Workforce Race Equality Standard (WRES) was introduced to the NHS in April 2015 to ensure that employees from black and minority ethnic (BME) backgrounds have equal access to career opportunities and receive fair treatment in the workplace.

The WRES is an integral part of the NHS Long Term Plan (LTP) and NHS People Plan, with ambitions for NHS trusts to set aspirational targets for BME representation across their leadership team and broader workforce. A model employer; *Increasing black and minority ethnic representation at senior levels across the NHS,* sets out the ambitions for this criterion to be met.

The aspirational targets have been developed by analysts at NHS England and the Department of Health and Social Care; they are based upon a robust and fit for purpose methodology.

To support this NHS England receives aggregate data (numbers) that are collected by NHS Digital from trusts under directions from the Secretary of State for Health and Social Care.

Working with the seven NHS England regional directors and their respective HR directors, individual organisation targets will be shared for oversight on how trusts in each region are performing against their objectives.

Aspirational target data for NHS trusts will not be published by the WRES team or regional teams, however individual organisations could publish their data if they choose to.

Payroll and Pensions Administration (NHS Payroll Services (NHS PS))

The payroll of NHS England is managed by NHS Payroll Services (NHS PS). Your personal information will be made available to NHS PS through the Electronic Staff Record (ESR) (see below) in order to allow them to pay your salary, any associated expenses, to make appropriate deductions and to comply with our legal and statutory obligations. From time to time we may need to share additional information to that held in ESR with NHS PS in order to ensure that they deliver the services we require and continue meet statutory or contractual obligations. Data will also be shared with pensions providers, e.g. NHS Pensions and NEST.

Electronic Staff Record (ESR)

Your personal information may also be used to fulfil other employer responsibilities, for example, by to maintain appropriate occupational health records, comply with health and safety obligations, carry out any necessary security checks and all other employment related matters. In addition, the information held may be used in order to send to you, information which is relevant to our relationship with you. Your information will only be disclosed as required by law or to our appointed agents and/or service providers who may be used for a variety of services, for example, processing of payroll and provision of pensions administration or staff surveys.

IBM, who provide ESR, and its partners as service providers will be responsible for maintaining the system. This means that they may occasionally need to access your staff record, but only to ensure that the ESR works correctly. Where this happens, access will be very limited and is only to allow any problems with the computer system to be investigated

and fixed as necessary. They will not have the right to use this data for their own purposes and contracts are in place with the Department of Health to ensure that the data is protected and that they only act on appropriate instructions. IBM and the ESR Central Team may access anonymised data about transactions on the ESR system to support the development and optimal use of the system.

Some of your personal information from ESR will be transferred to a separate database, known as the Data Warehouse. This will be used by various Government and other bodies (listed below) to meet their central and strategic reporting requirements. It will allow them to access certain personal information to generate the reports that they need and are entitled to. The Data Warehouse is intended to provide an efficient way of sharing information. Organisations currently granted access to the Data Warehouse are; NHS Digital, NHS Employers, Health Education England and its local committees (LETBs), Deaneries, Department of Health, Welsh Government, NHS Wales Shared Services Partnership, Care Quality Commission, NHS Trust Development Authority, and Monitor. The government may allow further organisations to have access in the future and therefore an exhaustive list cannot be provided, however any organisation having access to your data will have a legal justification for access.

Occupational Health Service Provider

The NHS England Occupational Health Service is managed by an external provider. Your personal information will need to be shared with the provider as and when required to allow them to provide NHS England employees and managers with the services required.

Expenses system provider

To provide an efficient way for staff to claim expenses, we use a hosted third-party software. Staff data is transferred to and from this system from the ESR system to ensure staff are able to claim and be reimbursed for expenses and NHS England can be assured this is within the policy set. The provider meets the ISO27001 information security standard in respect of the security of the data it holds. The provider processes the data to advise accurate amounts for reimbursement. The company may also periodically analyse the data to review trends and suggest improvements to NHS England.

Internal Audit

We provide information to our internal audit function, which is provided by an external service provider, to ensure NHS England has good processes and systems to manage and protect public funds.

Survey Providers

We may provide limited information to third party survey providers , to collect views from our staff and report on staff engagement within the organisation.

Flexible Working

We process personal data that is necessary to enable flexible working applications to be reviewed and progressed. This includes employee name, employee number, pay band, job title and the reason for requesting flexible working. This is received by the People and Organisational Development team who review the application.

Benefits system provider

We aim to provide our staff with employment benefits such as, gym opportunities, cycle to work scheme and other discounts to support staff personally and professionally whilst in employment with NHS England. NHS England's benefits system is managed by an external provider and your personal information will need to be shared with the provider as and when required to allow them to support you with the services you wish to take.

Other Bodies

NHS England is responsible for protecting the public funds it manages. To do this we may use the information we hold about you to detect and prevent crime or fraud. We may also share this information with other bodies that inspect and manage public funds. We may also share your personal information due to:

- Our obligations to comply with current legislation
- Our duty to comply with any Court Order which may be imposed

Any disclosures of personal data are always made on case-by-case basis, using the minimum personal data necessary for the specific purpose and circumstances and with the appropriate security controls in place. Information is only shared with those agencies and bodies who have a "need to know" or where you have consented to the disclosure of your personal data to such persons.

We will not routinely disclose any information about you without your express permission. However, there are circumstances where we must or can share information about you owing to a legal/statutory obligation or other legal basis for disclosure .

We may obtain and share personal data with a variety of other bodies, which may include:

- Her Majesty's Revenue and Customs (HMRC)
- Disclosure and Barring Service
- Home Office
- Child Support Agency
- Internal Audit, service currently provided by Deloitte LLP
- NHS Counter Fraud Authority
- Department of Health
- Central government, government agencies and departments
- Other local authorities and public bodies
- Ombudsman and other regulatory authorities
- Courts/Prisons
- Financial institutes for e.g. banks and building societies for approved mortgage references
- Credit Reference Agencies
- Utility providers
- Educational, training and academic bodies
- Law enforcement agencies including the Police, the Serious Organised Crime Agency
- Emergency services for e.g. The Fire and Rescue Service
- Auditors e.g. Audit Commissioner
- Department for Work and Pensions (DWP)
- The Assets Recovery Agency
- Relatives or guardians of an employee where there is a legal duty to do so

What if the data you hold about me is incorrect?

It is important that the information which we hold about you is up to date. If you believe that the information we hold is incorrect, in the first instance please check if the information can be updated on ESR through the Employee Self Service portal. Guidance is available at: https://nhsengland.sharepoint.com/TeamCentre/TCO/People/Pages/Workforce.aspx

If you are unable to make the change in ESR then please let us know by contacting your line manager and / or the Workforce Systems Team on england.workforcesystems@nhs.net.

Legal basis for processing

For entering into and managing contracts with the individuals concerned, for example our employees the legal basis is Article 6(1)(b) – ‘processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract’.

Where we have a specific legal obligation that requires the processing of personal data, the legal basis is Article 6(1)(c) – 'processing is necessary for compliance with a legal obligation to which the controller is subject'.

For other processing of personal data about our employees, our legal basis is Article 6(1)(e) – '…exercise of official authority…'.

For the additional processing of personal data about our employees in relation to the FPPT, our processing is also for the purposes of our legitimate interests. Further details around the FPPT can be found on the NHS England website and the significance of the information required which also helps align NHS England with other NHS bodies captured by the FPPT under Regulation 5 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2018.

Where we process special categories data for employment purposes the condition is:

Article 9(2)(b) – '…processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law…'.

Additionally, under our obligations as an employer and public authority, in relation to the FPPT; special category data is processed under Article 9(2)(g) – 'processing is necessary for reasons of substantial public interest…'.

For the processing of information about the health of our workforce, the legal basis is: Article 9(2)(h) – ' …processing is necessary for the purposes of preventive or occupational medicine…assessment of the working capacity of the employee…the provision of health or social care…'.

How the NHS and care services use your information: the National Data Opt-Out

Find out about how your information may be used for purposes beyond your individual care and how to register your choice to opt out.

NHS England is one of many organisations working in the health and care system to improve care for patients and the public.

Whenever you use a health or care service, such as attending Accident & Emergency or using Community Care services, important information about you is collected in a patient

record for that service. Collecting this information helps to ensure you get the best possible care and treatment.

The information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

- improving the quality and standards of care provided
- research into the development of new treatments
- preventing illness and diseases
- monitoring safety
- planning services

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is **only used** like this where allowed by law.

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt-out your confidential patient information will still be used to support your individual care.

Most of the time, anonymised data is used for research and planning so that you cannot be identified in which case your confidential patient information isn't needed.

To find out more or to register your choice to opt out, please visit www.nhs.uk/your-nhs-data-matters. On this web page you will:

- See what is meant by confidential patient information
- Find examples of when confidential patient information is used for individual care and examples of when it is used for purposes beyond individual care
- Find out more about the benefits of sharing data
- Understand more about who uses the data
- Find out how your data is protected
- Be able to access the system to view, set or change your opt-out setting
- Find the contact telephone number if you want to know any more or to set/change your opt-out by phone
- See the situations where the opt-out will not apply

You can also find out more about how patient information is used at:

- NHS Health Research Authority (which covers health and care research); and

- Understanding Patient Data (which covers how and why patient information is used, the safeguards and how decisions are made).

You can change your mind about your choice at any time.

Data being used or shared for purposes beyond individual care does not include your data being shared with insurance companies or used for marketing purposes and data would only be used in this way with your specific agreement.

The mandatory implementation of the National Data Opt-Out (NDOO), deadline of 31 March 2022, has been extended until 31 July 2022. We do not intend to extend implementation of the deadline any further.

As set out in the Operational Policy Guidance, the opt-out applies to the disclosure of confidential patient information for purposes beyond an individual's direct care across the health and care system in England, unless an exemption has been granted.

Organisations will be expected to take note of this new deadline and ensure they are taking the relevant steps to prepare to implement the opt-out by this date.

The following processing for which NHS England is a data controller, are exempt from the national data opt-out:

- Collection of personal data is required under s. 259 of the Health and Social Care Act 2012 following a Direction from NHS England or the Secretary of State. Information about the collections we have directed can be found on our website.
- Collection of confidential patient information about people with learning disabilities and/or autism who are in hospital for mental and/or behavioural healthcare reasons which is disclosed under the following approval under the Control of Patient Information Regulations 2002: Assuring Transformation: Enhanced Quality Assurance Process Data flow (CAG 8-02 (a-c)/2014). These flows continue to operate a separate opt-out mechanism and details of how to opt-out of the Assuring Transformation data collection can be found on the NHS England webpages. This exemption is time limited until the end of the "Building the Right Support Programme". The validation of invoices for non-contracted activities commissioned by NHS England or CCGs and for contract challenges where commissioners need to verify payment requests from care providers.
- The NHS England National Cancer Patient Experience Survey , the Under 16 Cancer Patient Experience Survey, and the National Diabetes Experience Survey, and the

Integrated Care Experience Survey. These national surveys will continue to operate separate opt-out mechanisms and details of how to opt-out of these surveys are provided by the relevant organisations undertaking the surveys.

Public Health

Information about the transfer of public health functions from Public Health England to NHS England

Transfer of Public Health functions to NHS England

On 1 October 2021, as part of the government's strategy to transform the public health system in England, responsibility for a number of public health functions transferred from Public Health England (PHE) to NHS England. NHS England is now therefore the controller for personal data processed to support these functions under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Other than the change in Controller there was no changes to patients' personal data to discharge these functions, how it is processed or the services received by patients as a result.

More information on NHS England's public health functions and commissioning activities can be found on our website.

Information about how we process personal data for the purposes of our screening programmes can be found at National population screening programmes: the information we use and why, and your options - GOV.UK (www.gov.uk).

From January 2023 the responsibility for the management of the National Disease Registries, a collection of data on all cancers, rare diseases and congenital anomalies diagnosed each year in England from NHS Digital to NHS England the privacy information can be found here National Disease Registration Service: NHS Digital Transparency Notice - NHS Digital.

Purposes for Processing

We process personal information of staff transferring into NHS England for the purposes of staff employment. Please see Our Workforce section of our privacy notice to find out how we use personal data about our employees.

We use personal information to fulfil the Secretary of State for Health and Social Care's duty to protect and improve public health and reduce health inequalities. We may process personal information in order to provide:

- Regional and National Healthcare Public Health services
- Regional and Local Screening functions and Immunisation Commissioning Support and Expert Advice
- Screening Quality Assurance Services

How we collect your personal information

We collect personal information from the following sources:

- Directly from you
- From the providers of health and care services
- From other organisations supporting the health and care system in England
- From national data sources including
    - The Office for National Statistics
    - The National Child Mortality Database
    - The National Disease Registration Service

The information we collect

The types of personal information we may collect about you include:

- Demographic information – for example, we may collect your name, date of birth, sex, ethnic group, NHS number, address and postcode, occupation, and contact details such as your phone number
- Health information – for example, we may collect information about your physical health, mental wellbeing, symptoms and medical diagnoses, and health risk factors such as your height and weight, whether you smoke and what your occupation is
- Treatment information – for example, we may collect information about your hospital admissions, clinic attendances, screening appointments, laboratory test results, prescriptions and vaccination history.

Who we share your information with

We may share your personal information with other organisations to provide you with individual care or for other purposes not directly related to your health and care.

- Your doctor and hospital to help them provide you and other patients with better care by auditing and evaluating the safety and effectiveness of the service they provide
- Data processors: We may share your personal information with organisations we have contracted to help us fulfil our remit

- With other organisations, where such sharing is necessary, proportionate and allowed by law, which may include universities and other researchers.

Legal basis for processing

We process both personal data and special categories of personal data, including data about your health and ethnic group. Our legal basis to collect your personal information may vary according to the purpose we use it for. In most cases unless stated below Section 7A of the National Health Service Act 2006 satisfies the UK General Data Protection Regulation and the Data Protection Act 2018 that apply below:

- GDPR Article 6(1)(e) 'processing is necessary for the performance of a task carried out in the exercise of official authority vested in the controller'
- GDPR Article 6(1)(a) 'consent' where processing for surveys and public consultations for changes

Where we need to use special categories of personal data, the lawful bases will be:

- GDPR Article 9(2)(i) 'processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health'
- GDPR Article 9(2)(h) 'processing is necessary for the provision of health or social care or treatment or the management of health or social care systems and services'
- GDPR Article 9(2)(a) 'explicit consent'
- Data Protection Act Schedule 1 Part 1 (3) 'public health'

Former NHS Improvement Functions

Information about the transfer of functions from Monitor and the NHS Trust Development Authority to NHS England

The 2022 Health and Care Act introduced new legislative measures that aim to make it easier for health and care organisations to deliver joined-up care for people who rely on multiple different services, building on earlier recommendations by NHS England and NHS Improvement.

The Health and Care Act 2022 created a single NHS Organisation comprising what was previously Monitor and NHS Trust Development Authority (TDA), known as NHS Improvement. As of 1 July 2022 a number of the processes and functions formerly undertaken by Monitor and the NHS Trust Development Authority are transferred to NHS England.

We have set out below a description of all the ways we process your personal data for those processes and functions transferred to NHS England, and the legal bases we rely on to do so.

Ambulance Service Records

Purposes for Processing

To securely store ambulance service records which are unable to be repatriated due to closure of the service

Type of Data

(a) Identity (b) Contact (c) Special categories

Lawful basis for processing including basis of legitimate interest

Necessary for our legitimate interests to ensure secure storage of unrepatriated ambulance service records. Necessary for reasons of substantial public interest.

Recruitment for NHS Trusts and Charities

Purposes for Processing

To recruit, appoint, appraise and develop executives, chairs and non-executive directors to NHS trusts and trustees to NHS charities, and support NHS foundation trusts in recruiting executives, chairs and non-executive directors

Type of Data

(a) Identity (b) Contact (c) Special Categories (d) Other personal data related to recruitment

Lawful basis for processing including basis of legitimate interest

Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in NHS England.

Necessary for the management of health or social care systems and services – health and social care purposes.

Capacity, Capability and Diversity Monitoring

Purposes for Processing

To improve the leadership of NHS trust and foundation trust boards by monitoring their capacity, capability and diversity

Type of Data

(a) Identity (b) Contact (c) Special Categories

Lawful basis for processing including basis of legitimate interest

Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in NHS England.

Necessary for our legitimate interests to ensure diversity in recruitment.

Necessary for the management of health or social care systems and services — health and social care purposes

Research Programmes

Purposes for Processing

To improve the leadership of NHS trust and foundation trust clinical staff through research programmes

Type of Data

(a) Identity (b) Contact

Lawful basis for processing including basis of legitimate interest

Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in NHS England

Compliance with NHS Provider Licence

Purposes for Processing

To monitor independent providers' compliance with the NHS Provider Licence

Type of Data

(a) Identity (b) Contact

Lawful basis for processing including basis of legitimate interest

Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in NHS England

Applications for NHS Provider Licence

Purposes for Processing

To process applications for the NHS providers' licences and process requests for the revocation of an NHS provider licence

Type of Data

(a) Identity (b) Contact

Lawful basis for processing including basis of legitimate interest

Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in NHS England

Getting It Right First Time Programme

Purposes for Processing

Information for Getting It Right First Time Programme

Type of Data

(a) Identity (b) Contact (c) Special Categories

Lawful basis for processing including basis of legitimate interest

Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in NHS England

Necessary for the management of health or social care systems and services – health and social care purposes

NHS England Nurses' Data

Type of Data

(a) Contact

Lawful basis for processing including basis of legitimate interest

Explicit Consent

Theatre Productivity Programme

Purposes for Processing

Theatre productivity programme (clinician-level activity data)

Type of Data

(a) Identity (b) Contact

Lawful basis for processing including basis of legitimate interest

Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in NHS England

Healthcare Safety Investigation Branch (HSIB)

Type of Data

(a) Identity (b) Special Categories

Lawful basis for processing including basis of legitimate interest

Explicit consent

Necessary for reasons for substantial public interest

Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in NHS England

Necessary for the management of health or social care systems and services — health and social care purpose

National Clinical Improvement Programme

Purposes for Processing

National Clinical Improvement Programme; to set up user accounts for consultants and create the database containing consultant level patient pseudonymised clinical activity data sourced from Hospital Episode Statistics (HES) provided by NHS Digital

Type of Data

(a) Identity (b) Contact (c) Special Categories

Lawful basis for processing including basis of legitimate interest

Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in NHS England

Necessary for delivering our statutory functions

Necessary for the management of health or social care systems and services – health and social care purposes.

NHS England, NHS Digital and Health Education England Merger

In November 2021 the then Secretary of State for Health and Social Care set out their intention to merge Health Education England with NHS England, and also accepted a recommendation from the Chair of NHS Digital to merge NHS Digital and NHSX with NHS England with an expected legal merger date of 1st April 2023.

To prepare for the merger with NHS England and Health Education England, personal data about our staff will need to be shared with the other organisations involved in the merger.

Purposes for processing

- **Organisational design work** – to design the future shape and structure of the new NHS England.

- **Communications and engagement** – your work email addresses will be shared so that you can receive important communications about the merger, including invitations to All Colleague Briefings.
- **Consultations** – to meet legal requirements for staff consultation
- **Equality Impact Analysis** – to conduct Equality Impact Analysis, only aggregate anonymous data related to protected characteristics will be used for this purpose. Small numbers will be suppressed so that no individual can be identified from this data.
- **Access to ICT systems –** your work email address will be used to provide you with guest access to NHS England's systems such as the Expressions of Interest (EIO) system to apply for vacancies, and the Creating the New NHS England Microsite to access key information and resources relating to the merger.
- **Provision of voluntary redundancy schemes –** staff NHS employment history, length of service and salary information will be used as a resource for the provision of voluntary redundancy schemes.

Sources of data

All data originates from Health Education England, NHS Digital and NHS England.

Categories of personal data and recipients

The following categories of personal data will be shared from your Electronic Staff Record (ESR):

- Your contact information (e.g. Your first name, surname, work email address)
- Your employment information (e.g. Your employment number, assignment number, job title, office location, start date, contracted hours, details of previous NHS service.)
- Your grade and salary information (e.g. Your pay grade, salary, spinal value, pay step date)

In order to carry out equality impact analysis, in accordance with the Equality Act 2010, we will be sharing anonymous and aggregated information about our employees' protected characteristics. Those characteristics include colleagues' age, pregnancy and maternity, marriage and civil partnership, disability, race, religion or belief, sex and sexual orientation. This information will only be shared in an anonymous and aggregated form so none of our colleagues will be identifiable from the information which is shared. From the anonymous data small numbers, which relate to a small number of individuals, will be suppressed.

Your personal data will be shared with a limited number of individuals in NHS England, Health Education England and NHS Digital who require access to identifiable data to perform their role relating to the merger. Where the task they are performing does not require access to identifiable data, only access to aggregate anonymous data will be provided.

Personal data will be stored within the Foundry platform (Palantir acting as data processor) for the provision of the above purposes.

NHS England has also instructed the following organisations;KPMG, PA Consulting and McKinsey & Company, who will be acting as data processors to NHS England for this purpose, to provide support and assistance to the activities which are required to facilitate the merger. These organisations will only be given access to personal data which they require to complete the tasks assigned to them by NHS England. They cannot use the data they have been given access to for any other purposes.

Legal basis for processing

Under the UK General Data Protection Regulation (UK GDPR) our legal basis to share data from your ESR record is:

- **Contract** – Article 6(1)(b) of UK GDPR in relation to your contract of employment
- **Legal obligation** - Article 6(1)(c) of UK GDPR in relation to the Equality Act 2010, execution of the Public Sector Equality Duty and legal requirements for consultation
- **Public task** - Article 6(1)(e) of UK GDPR in relation to carrying out the required activities and tasks needed to merge the three organisations to create the new NHS England.

We also need an additional legal basis in the UK GDPR and the Data Protection Act 2018 (DPA 2018) to use data which is particularly sensitive. NHS Digital will need to process sensitive data about employees' protected characteristics to transform that data into aggregate and anonymous data before it is shared with NHS England and Health Education England for the purposes of equality impact analysis. Our legal basis to handle this sensitive data to make it anonymous is:

- **Employment purposes** – Article 9(2)(b) of UK GDPR, plus Schedule 1, Part 1, Paragraph 1 "Employment, social security and social protection" of DPA 2018
- **Substantial public interest** – Article 9(2)(g) of UK GDPR, plus Schedule 1, Part 2, Paragraph 8 "Equality of opportunity or treatment" of DPA 2018

NHS Federated Data Platform Privacy Notice

This Privacy Notice provides information about the processing of Personal Data in the NHS Federated Data Platform (FDP).

For more information about the FDP, please see the dedicated webpages about FDP and the Frequently Asked Questions.

This Privacy Notice provides answers to the following questions about the processing of Personal Data in the FDP:

1. What is the NHS Federated Data Platform (“**FDP**”)?
2. When will the FDP start being used?
3. What type of data is processed in the FDP?
4. Who is responsible for processing data in the FDP
5. What are the purposes for processing Personal Data in the FDP?
6. Where does the data processed in the FDP come from?
7. Who has access to data in the FDP?
8. How is data protected in the FDP?
9. How long will the data in the FDP be kept for?
10. Where is data held in the FDP stored?
11. What are my data protection rights in relation to Personal Data processed in the FDP?
12. What are the legal grounds to process Personal Data in the FDP under data protection law?
13. Do opt-outs apply to data processed in the FDP?
14. Questions, feedback, concerns and your right to make a complaint.
15. Changes to this Privacy Notice.

What is the NHS Federated Data Platform (“FDP”)?

Data is a core part of how the NHS delivers care, it’s at the heart of transforming services and improving outcomes for patients; using it well saves lives.

The NHS Long Term Plan highlights the importance of technology in the future NHS; setting out the critical priorities that will support digital transformation and provide a step change in the way the NHS cares for citizens.

People, data and technology are crucial to the ongoing evolution of the NHS. Working together in these key areas will support and enable local NHS organisations to:

- work in more efficient ways,
- improve diagnosis and treatment,
- improve services.

A key enabler for this is the roll-out of the NHS Federated Data Platform.

The NHS uses data every day to manage patient care and plan services. Historically, it's been held in different systems that don't always speak to each other, creating burden for staff and delays to patient care. The Federated Data Platform is a solution to that problem. The FDP brings data together from existing IT systems to enable staff in an NHS organisation to access the information that their own IT systems already hold in a single, safe and secure place.

The NHS Federated Data Platform

The NHS Federated Data Platform is made up of a number of separate independent data platforms, each of which is called an "**Instance**" alongside transparency and privacy enhancing technology, which is called "**PET**". Together, we call the different Instances and PET the "**FDP**" in this Privacy Notice.

Some Instances are operated by NHS England and are called "**National Instances**". There are also separate Instances which are operated by an NHS trust or an integrated care board in a local area, which we call "**Local Instances**".

We call each of these organisations "**User Organisations**" in this Privacy Notice.

Privacy Enhancing Technology or PET

The National and Local Instances work alongside PET. PET is transparency and privacy enhancing technology which has two functions:

1. **Registering data flows** - PET creates records of the types and uses of data which are used in every Instance of FDP. We call this "**registering**" the data. PET does not process the Personal Data to do this. From March 2024 when the FDP starts to be rolled out, PET will be integrated into all Instances and will register all data being used in the FDP.
2. **Treating Personal Data** - PET can also be used to de-identify Personal Data. This involves processing Personal Data. PET will not initially process Personal Data to de-identify it. This will however start to be done in phases from Summer 2024.

Products

Each Instance of the FDP uses the same underlying technology and software and has the same basic technical functionality. However, the FDP uses the technology, software and functionality in different ways for different purposes in specific "**Products**".

Some Products are only designed to be used in the National Instances, some are only designed for the Local Instances, and some are designed to be used in both types of Instance.

A Product is a software solution for a particular NHS need. Each Product will process only the data which is the minimum necessary to meet that NHS need. Most Products that will be used in Local Instances will be designed to help clinicians to provide care and treatment to their patients. This means that information that identifies their patients who are receiving care and treatment will be used in the Local Instances.

Most Products that will be used in the National Instances will be designed to help NHS England, NHS Trusts and Integrated Care Boards to understand how the NHS is operating and to plan and manage how they deliver healthcare services safely and effectively. Where a Product that is used in the National Instances is also to be used by an NHS Trust or Integrated Care Board, then it will also be available in their Local Instance. Most Products in the National Instances will only need to use data that does not identify individuals, because NHS England doesn't usually need data that identifies specific patients to help plan, commission and manage health care.

Although each Instance of the FDP is separate from other Instances, where it is agreed that data can be shared across Instances, the Products used in FDP can provide a safe and secure way to share relevant information. This is known as federation.

Sharing data across Instances will only happen within a Product where this is necessary for organisations to work together to provide care directly to patients or to manage and plan how care is delivered to patients. Data will only ever be shared where it is allowed under data protection laws.

When will the FDP start being used?

The FDP is being rolled out to User Organisations in implementation Phases.

Transition Phase: March 2024 – May 2024

The first Phase is the "**Transition Phase"**, which involves NHS England, NHS Trusts and Integrated Care Boards who currently use Products, moving their existing Products onto the new version of the software that is in FDP. There is no change to the data that is being processed, the purposes for which it is processed or the User Organisations who are processing the data during the Transition Phase.

The Transition Phase will start in March 2024 and is expected to run until May 2024. It will consist of 5 Waves, starting with Wave 0 and finishing with Wave 4. Each Wave will consist of a number of existing User Organisations and existing Products which will transition to FDP. This is organised in Waves to manage the transition process.

Delivery Phase: May 2024 – March 2027

The Delivery Phase is expected to start in May 2024 and run through to March 2027. Following a successful transition of existing User Organisations and Products to FDP, FDP will be rolled out more widely in the NHS. This will involve rolling out:

- Existing local Products to new User Organisations in Waves.
- The use of PET to process Personal Data to de-identify it and to replace legacy NHS de-identification solutions.
    - PET will be used to support Products which require Personal Data to be de-identified for them to be used for the purpose of the Product. This will apply to National Products. Currently there are no Local Products which require Personal Data to be de-identified for them to be used.

    - This will be a staged process and is expected to commence from summer 2024 and continue until 2026.
- New Products to User Organisations

During the implementation of FDP, this Privacy Notice and the Product Privacy Notices will be regularly updated to list the Products and User Organisations who are using FDP and also when PET starts to process Personal Data.

What type of data is processed in the FDP?

Types of data

Data means items of information. There are two main types of data that are processed in the FDP:

Personal Data

Personal Data is defined in data protection law and is information relating to a living individual that can directly or indirectly identify them. Personal Data can be either:

- **Directly Identifiable Data** – this is Personal Data that can directly identify an individual, for example, a name.
- **De-Identified Data** – this is Personal Data that has been de-identified, so that an individual can no longer be directly or indirectly identified in the data, but where the organisation holding the data does still have the means to identify the individual.

Individuals have a number of rights under data protection law in relation to their Personal Data.

Categories of Personal Data

Personal Data that is processed in the FDP will include information that identifies an individual, including basic information about such as a name, address, date of birth and contact details, and information about the individual's health and treatment.

The items of Personal Data that may be processed vary depending on the Product and the purposes for which they are being processed. Each Product will process only the data which is the minimum necessary to meet the NHS need.

Level 3 – Personal Data that is processed in the FDP varies depending on the Product and the purposes for which the data is processed. Personal Data that identifies an individual will be used in local Instances, as the Products used by NHS Trusts and Integrated Care Boards bring data together which is used to provide those individuals with care and treatment. In the national Instances of FDP, most Personal Data will not include information that directly

identifies individuals as it will have gone through a process called pseudonymisation, which means that the data will be referred to as De-Identified Data.

Local Instances

Directly Identifiable Data is processed in Local Instances as most Products enable clinicians to provide individual care to patients who they treat. Access to this information is still restricted to only the information that a clinician and their care team need to know for the specific purpose of providing care to an individual. This information may include an individual's:

- name
- address
- date of birth or age
- gender
- sex
- NHS number or hospital record number
- telephone number
- email address
- marital status
- health information, including information about their symptoms, medical conditions, diagnosis, medication and treatment
- race and/or ethnicity
- religious and/or other beliefs
- sexual life and/or sexual orientation (where this is relevant to their care)
- living arrangements, living habits and diet
- genetic information

National Instances

De-Identified Data processed in Products within the national Instances will be used by NHS England to understand how the NHS is operating and to help NHS Trusts and Integrated Care Boards to plan and manage how they deliver care to patients.

For example, De-Identified Data is used by NHS England analysts to produce dashboards which share Anonymous Aggregated Data (which is defined below) with users of the dashboard. Only the minimum amount of De-Identified Data that is necessary for the specific purpose of producing the dashboard is used in a Product. Access to the data is strictly controlled. In most cases only analysts within NHS England will have access to the De-Identified Data in national Products, so they can create and maintain the dashboard. Most users of the dashboard will only be able to see Anonymous Aggregated Data and Operational Data that is displayed to them in the dashboard.

De-Identified Data does not directly identify any individuals, so it does not include a name or contact details. It may include information about:

- the area they live in
- their age
- their gender or sex
- their race or ethnicity
- their care and treatment including information about hospital admission and stays, health conditions, diagnosis, treatment, discharge, and their outcome from treatment.

More information about the specific categories of Personal Data that are processed in each Product are contained in the Product Privacy Noticesv.

Personal Data will only be processed in FDP where it is strictly necessary for the specific purpose it is being used for. NHS staff who are using FDP are subject to strict confidentiality rules and FDP will only allow them to see the items of Personal Data which they need to see for the purposes for which they are using the data. Where they don't need to know who an individual is, FDP will restrict their access to De-Identified Data or Anonymous Data (which is defined in the section below).

Each organisation using FDP will decide which members of staff can see specific types of information in line with data protection requirements, by using access control rules that are implemented within the FDP to strictly minimise access to only data that is necessary for a particular purpose.

Anonymous Data

This is data that does not relate directly to individuals. It can be either:

- **Anonymised Data** – this is data which may have been Personal Data, but that has been de-identified so it no longer directly or indirectly identifies an individual. Data is anonymous when it is not reasonably possible for the organisation or the person using the data to re-identify the individual.
- **Aggregated Data and Operational Data** – this is data that does not relate directly or indirectly to specific individuals.

For example, statistics about groups of individuals where no one can identify any specific individuals from the statistics eg, numbers describing the stocks of medicine, or the number of beds in a hospital.

Data protection law does not apply to Anonymous Data.

The type of data and categories of Personal Data that are processed in FDP vary in relation to each Product used on FDP. More information about each Product and the data that is processed in them is available in Section 5 below.

Who is responsible for processing data in the FDP?

NHS England, and a number of NHS Trusts and Integrated Care Boards, are using the FDP and each has their own data protection responsibilities for the data they process in FDP. Each of these organisations is a User Organisation. The full list of User Organisations using the FDP, including the Products they are using is here.

What are the responsibilities of User Organisations under data protection law?

Under data protection law, each User Organisation is the '**Controller**' for the Personal Data it processes in its Instance. As a Controller, each User Organisation makes decisions about how to use the FDP, which Products it wants to use in its own Instance, and what Personal Data it needs to put into the FDP, to use those Products.

NHS England is the Controller for the Personal Data which is processed within the National Instances.

Each NHS Trust or Integrated Care Board is the Controller of the Personal Data which is processed within its Local Instances.

NHS England, and each NHS Trust or Integrated Care Board, are also joint Controllers for some aspects of how the FDP operates.

Level 3 - NHS England and each NHS Trust or Integrated Care Board are also joint Controllers in relation to the design, governance, and service management of the local Instances of FDP. This is because together NHS England and each User Organisation has decided to use FDP and the functionality it has been designed to provide. They have also agreed to work together to put in place governance arrangements for how FDP is used by each User Organisation. NHS England and other User Organisations have also agreed that because NHS England has entered into the contracts with the contractors who have designed and operate the FDP, that NHS England will be responsible for managing those contracts.

More information about who is responsible for elements of processing which are subject to joint control is set out in Section 9 and 26 of the Overarching FDP Data Protection Impact Assessment.

What are the purposes for processing Personal Data in the FDP?

At present, all User Organisations have agreed only to use FDP for purposes that fall within five broad NHS priority purposes, which we call "**Use Cases**". All Products which are used by the FDP therefore must also fall within one of these Use Cases. The five current Use Cases are:

- **Population Health and Person Insight** – to help integrated care systems proactively plan services that meet the needs of their population.

- **Vaccination and Immunisation** – to continue to support the vaccination and immunisation of vulnerable people whilst ensuring fair and equal access and uptake across different communities.
- **Elective Recovery** – to address the backlog of people waiting for appointments or treatments which has resulted from the COVID-19 pandemic alongside Winter pressures on the NHS.
- **Care Coordination** – to enable the effective coordination of care between local health and care organisations and services, reducing the number of long stays in hospital.
- **Supply Chain** – to help the NHS put resources where they are need most and buy smarter so that we get the best value for money.

In future User Organisations may agree that FDP can be used to meet other Use Cases. NHS England has agreed to consult with patient groups and other organisations, including the National Data Guardian and the Information Commissioner's Office, before any other Use Cases are agreed.

More information about the purposes for which each Product processes Personal Data and under which Use Case, can be found on the NSH England website: NHS England » NHS Federated Data Platform (FDP).

For example, one of the Products which will be used by NHS Trusts in Local Instances of the data platform from Wave 1 is called The Optimised Patient Tracking and Intelligent Choices Application (OPTICA).

The Product is integrated with a hospital's electronic patient records and, combined with other local health and social care data systems, ensures that relevant information related to patient discharges is available to clinical teams and leaders, in one place, as a single version of the truth.

This is a Product that tracks all admitted patients and the tasks and blockages relating to their discharge in real-time through their hospital journey. The Product is helping ensure that patients who no longer need to be in hospital can go home, or into appropriate community services with relevant support, as quickly as possible.

This Product falls within the Care Co-ordination Use Case.

There is a video here which provides more information about the benefits of using this Product for patients and staff.

Where does the data processed in the FDP come from?

The Personal Data processed in the FDP is Personal Data that is already held in local IT systems or is shared back with local IT systems and is processed by each User Organisation in accordance with data protection laws.

In the case of NHS Trusts, the Personal Data that is brought into the FDP will be Personal Data taken from other hospital systems, such as theatre scheduling systems and electronic patient record systems. In some cases, the Product will generate some new information, for example a hospital discharge summary, and that information will be shared back into the electronic patient record system by the local NHS Trust.

In the case of NHS England, the Personal Data processed in the FDP will be Personal Data that NHS England has already collected from NHS Trusts and currently processes in other NHS England data platforms, including the COVID-19 data platform.

Who has access to the data in the FDP?

Staff in a User Organisation

Staff who work for a User Organisation will only have access to the data in the FDP that they need to perform their specific job. In Local Instances, this will include doctors, nurses, administration staff supporting them, and administration staff and managers running the hospital.

Staff in other organisations

So that a hospital can provide you with the best care, it may need to share data about you that is processed in the FDP with other organisations. NHS England may also want to share Aggregated Data with your hospital or local Integrated Care Board to help them to plan and manage care they provide to their patients.

Any Personal Data that is shared with other organisations will be the minimum amount necessary. Individuals will only be identified if this is necessary for the purposes for which it is shared. For example, in a Product used in a Local Instance information about an individual may need to be shared with another organisation for the purposes of the individual's care. Personal Data can only ever be shared if there are legal grounds under the data protection laws that allow this.

Where possible, if data needs to be shared, this will be done within the FDP. Data will be shared with other User Organisations through the FDP by providing members of staff from other User Organisations with access to the data across Instances of the FDP.

For some Products, including in the National Instances, dashboards are produced which may be viewed by other organisations, including NHS Trusts and the Department for Health and Social Care, who are not User Organisations. Providing access to these dashboards through FDP will help keep the data secure.

In some cases, data may need to be shared outside of FDP. If this happens, logs of the data sharing will be kept by the FDP. These logs will register who the data was shared with and for what purposes. Only certain authorised users in a User Organisation will be able to approve data sharing with other organisations.

If the data is not being shared for individual care, and is Personal Data or Confidential Data, the User Organisations will only share data or provide access to view it, where there is a data sharing agreement in place.

Information about how data is kept secure in FDP, and when it is shared, is in Section 8 below.

Processors – FDP Contractors

There are two companies that together provide the software for the FDP and who operate and maintain this software for each User Organisation. NHS England appointed these two companies following a public procurement. Together we call these companies the "**FDP Contractors**".

They are:

- **Data Platform – Palantir Technologies UK, LTD.**
- **PET – IQVIA LTD**.

The FDP Contractors only process Personal Data in the FDP where it is necessary for them to operate and maintain the FDP (which we call "**FDP Services**") for User Organisations. Under data protection law they are called "**Processors**". This means that they can only process Personal Data on behalf of a User Organisation and for the purposes of providing these FDP Services. They must only act on the written instructions of the User Organisation. These written instructions are given under a data processing agreement between the FDP Contractor and each User Organisation for each Product that a User Organisation chooses to use.

If a Processor breaches the terms of its data processing agreement, or processes Personal Data outside of the instructions given by a Controller, this may breach data protection laws.

This may lead to the Information Commissioner taking regulatory action, including issuing a fine to a Processor who has broken the law.

The FDP Contractors are not allowed to appoint other contractors **("Sub-processors**") to work for them to process Personal Data to provide the FDP Services unless those Sub-processors have first been approved by User Organisations. A list of Sub-Processors that have been approved by User Organisations is on the NHS England website: NHS England » Sub-processors

The FDP Contractors and their Sub-processors are not allowed to use any Personal Data in the FDP for their own purposes, except some limited data, such as contact details, concerning User Organisation's staff which they need to provide the FDP Services.

How is data protected in the FDP?

The FDP has been developed with privacy at the centre of its design, ensuring that the protection and privacy of Personal Data has been considered through the design of FPD, into the implementation of the Products and in relation to the governance approach to using FPD.

Data is protected in a number of ways including:

- **Separation of Control** – The FDP is designed to work as separate Instances controlled by each User Organisation. Governance and technical controls are in place to ensure that no individual organisation or user has access to all data. NHS user roles are separated to ensure no individual has access to all data.
- **Separation of the Data Platform from PET** - PET is provided by a separate contractor from the supplier of the data platform. This means that where only De-Identified Data is needed for a particular Product, no Directly Identifiable Data needs to be shared into an Instance. It will be processed by the PET Contractor to remove identifiers before it is shared into the Instance. This service is expected to start from Summer 2024.
- **Role based access controls** - NHS user roles are defined and separated to ensure that staff are only able to access data they need to do their work.
- **Staff training** - All staff are required to complete mandatory data protection and security training in the NHS. In addition, staff will undergo training in the use of each Product, ensuring data is used appropriately and securely.

- **Data minimisation** – The FDP will only process the minimum data that is necessary for the purposes of a Product. This is assessed as part of a Data Protection Impact Assessment (DPIA) which is required under data protection laws where Personal Data is processed within FDP and is carried out as part of a User Organisation deciding to use a Product.
- **Transparency of data access and use** – PET will create records of all data entering and leaving the platform and its approved purposes of use.
- **Audit Logs –** All access and use of data in the FDP will be logged so that User Organisations can audit and review who has accessed what data in their Instance.
- **User authentication** – All user access to the FDP must be authenticated using multi-factor authentication.
- **Technical Security –** All data stored in the FDP will be protected via industry good practice layers of protection, including encryption of data stored in FDP and in transit (when it comes to FPD and leaves FDP), regular penetration testing, firewalls, anti-virus and intrusion protection.
- **Security Monitoring –** Cyber and security threats in FDP will be monitored by the FDP Contractors and by NHS England's Cyber Security Operations Centre.
- **Privacy Treatment** – PET will provide tools to de-identify Personal Data where Personal Data needs to be de-identified before it is used in a Product.

How long will the data in the FDP be kept for?

Data will be kept in the FDP for as long as it is necessary for a User Organisation to process it. This will depend on the Product the data is used in and the purposes for which the data is processed. The processing of all Personal Data, including the periods of time that data is kept, will be in accordance with the NHS Records Management Code of Practice 2021.

Where is data held in the FDP stored?

All data held in the FDP is securely stored on servers in the United Kingdom (UK).

What are my data protection rights in relation to Personal Data processed in the FDP?

Under data protection law, you have the following rights over your Personal Data:

- **Your right to be informed about how your Personal Data is used**– You have the right to be told how and why a User Organisation is processing your Personal Data.

This Privacy Notice has been published to explain how your Personal Data is being processed by all User Organisations. ("**Right to be informed**")

- **Your right to get copies of your Personal Data** – You have the right to ask a User Organisation that is processing your Personal Data in FDP for copies of your Personal Data (called a "**Right of access**").
- **Your right to get your Personal Data corrected** – You have the right to ask a User Organisation that is processing your Personal Data in FDP to correct ("**Right to rectify**") your Personal Data if you think it is inaccurate or incomplete.
- **Your right to get your Personal Data deleted** – You have a right to ask a User Organisation that is processing your Personal Data in FDP to delete ("**Right to erase**") your Personal Data in certain circumstances.
- **Your right to restrict how your Personal Data is used** – You have the right to ask a User Organisation that is processing your Personal Data in FDP to limit the way they use it (restrict processing) in certain circumstances ("**Right to restrict**").
- **Your right to object to how your Personal Data is used** – You have the right to object to a User Organisation about how your Personal Data is used in FDP in certain circumstances ("**Right to object**").
- **Your right of data portability** – You have the right to ask a User Organisation that is processing your Personal Data in FDP to transfer your Personal Data to another organisation or give it to you in certain very limited circumstances ("**Right of data portability**").
- **Your right to not have 'automated' decisions made about you by a User Organisation, including profiling –** You have the right not to have automated decisions made about you, including profiling, if the decision affects your legal rights or it has other significant effects on you.

To exercise your data protection rights, you should contact the Data Protection Officer for the User Organisation who is processing your Personal Data. A list of Data Protection Officer contact details for all FDP User Organisations is here: NHS England » FDP User Organisation Data Protection Officers

You can find out which specific data protection rights apply in relation to Personal Data processed in each Product in the Product Privacy Notices here: NHS England » NHS Federated Data Platform privacy notice

What are the legal grounds to process Personal Data in the FDP under data protection law?

User Organisations must have legal grounds under data protection law before they can use your data in FDP.

The Privacy Notices for each Product provide specific information about the legal grounds that apply to the processing of data in each Product which you can access here.

Personal Data

In general, User Organisations will rely on one or more of the following legal grounds to process Personal Data in the FDP under data protection law:

- **Legal obligation** - Article 6(1)(c) of UK GDPR.
- **Public task** - Article 6(1)(e) of UK GDPR

Special Category Personal Data

User Organisations also need an additional legal ground to process special categories of Personal Data under data protection laws. "**Special Category Data**" is:

- Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership,
- the processing of genetic data,
- biometric data for the purpose of uniquely identifying a natural person,
- data concerning health, or
- data concerning an individual's sex life or sexual orientation.

The legal grounds for processing Special Category Data under data protection law include:

- **Substantial public interest** – Article 9(2)(g) of UK GDPR, plus Schedule 1, Part 2, Paragraph 6 "statutory etc and government purposes" of the Data Protection Act 2018 ("**DPA 2018**")
- **Health or social care** – Article 9(2)(h) of UK GDPR, plus Schedule 1, Part 1, Paragraph 2 "Health or social care purposes" of DPA 2018
- **Public health** – Article 9(2)(i) of UK GDPR, plus Schedule 1, Part 1, Paragraph 3 "Public health" of DPA 2018

- **Statistical purposes** - Article 9(2)(j) of UK GDPR, plus Schedule 1, Part 1, Paragraph 4 “Research etc” of DPA 2018

Confidential Data

Personal information about an individual which has been provided in circumstances of confidence is called “**Confidential Data**”. This includes information that directly or indirectly identifies an individual and information about the health care and treatment of an identifiable individual. Additional rules apply when Confidential Data is processed by a User Organisation in the FDP and additional legal grounds will apply. More information about these rules and the legal grounds is here.

- Level 3 content – **Legal grounds for processing Confidential Data**
  Where Confidential Data is processed by User Organisations in the FDP, an additional legal ground will need to be identified so that the use of the Confidential Data does not breach confidentiality. These additional legal grounds are:
    - where it can be assumed that the individual has provided their consent (“**implied consent**”). The National Data Guardian’s guidance sets out that this legal ground only applies where the processing of Confidential Data in any particular circumstances is carried out for the purpose of the direct care of an individual,
    - where the User Organisation has a legal obligation to process the Confidential Data,
    - where there is a power in legislation to expressly process Confidential Data (“**statutory authority**”). This includes processing Confidential Data in relation to:
        - communicable diseases, such as coronavirus, under Regulation 3 of the Health Service (Control of Patient Information) Regulations 2002 (“**COPI Regulations**”), or
        - medical purposes approved by the Secretary of State with support from the Confidentiality Advisory Group under Regulation 5 of the COPI Regulations. This is also known as an approval under Section 251 of the NHS Act 2006, or
    - where there is an overriding justification which is in the public interest.

Do Opt-outs apply to data processed in the FDP?

Type 1 opt-outs – Do not currently apply to Products used in the FDP

A Type 1 opt-out registered with a GP Practice prevents an individual’s confidential patient information from being shared outside of their GP Practice except when it is being used for the purposes of their individual care.

Type 1 opt-outs do not apply to data processed in the FDP because:

- No confidential patient information that has come from a GP Practice is being processed by a Product in the National Instances of FDP.
- Confidential patient information that has come from a GP Practice which is being used in the FDP in a Product in a Local Instance is only being used for the purposes of individual care.

If this changes in the future because a new Product processes confidential patient information in a way which would mean that the Type 1 opt-out would apply, the relevant User Organisation would be responsible for ensuring that the Type 1 opt-out was applied and this Privacy Notice will be updated to make this clear.

National Data Opt-Out – Does not currently apply to Products used in the FDP

The National Data Opt-Out provides an individual with a right to opt out of their confidential patient information being used for purposes beyond their direct care, unless an exemption applies under the National Data Opt-Out Operational Policy Guidance.

The National Data Opt-Out does not apply to data processed in the FDP because:

- **National Instances** - No confidential patient information is being processed by a Product in the National Instances of FDP to which the National Data Opt-Out would apply.
- **Local Instances** - Confidential patient information that is being used in the FDP in a Product in a Local Instance is only being used for the purposes of direct care and therefore the National Data Opt-Out does not apply.

More information about why the National Data Opt-Out does not apply is set out in each Product Privacy Notice here.

You can find out more about and register a National Data Opt-Out or change your choice on nhs.uk/your-nhs-data-matters

Local opt-outs

NHS Trusts and Integrated Care Boards may have provided their patients with the right to opt out of their Confidential Data or Personal Data being used for specific purposes within their local area, eg within local shared patient record systems, for particular purposes.

More information about those local rights to opt-out will be provided in the relevant NHS Trust or Integrated Care Board Privacy Notices, which should be available on their websites.

It is the responsibility of the NHS Trust and Integrated Care Board to ensure that local opt-outs are implemented within the data that is shared into and processed in FDP where they apply.

Questions, feedback, concerns and your right to make a complaint

A lot of information is published about FDP on the NHS England website here.

If you have any questions about the FDP that you can't find the answer to on the website, or you want to leave feedback about any aspect of FDP, or you would like to register to take part in future FDP engagement activity, you can do this through the FDP Engagement Portal here: Home - NHS Federated Data Platform (england.nhs.uk)

If you have any concerns about how a User Organisation is using your Personal Data, please contact its Data Protection Officer. Details for each User Organisation's Data Protection Officer is here.

If you are not happy with the response from the Data Protection Officer, you have the right to make a complaint about how your Personal Data is being used in the FDP to the Information Commissioner's Office ("**ICO**"). You can do this by:

- calling 0303 123 1113
- using the ICO website: https://ico.org.uk/make-a-complaint/
- writing to:

  Information Commissioner's Office
  Wycliffe House
  Water Lane
  Wilmslow
  Cheshire
  SK9 5AF

Changes to this Privacy Notice

We will make changes to this notice to reflect the roll out of the FDP across the NHS and as new Products are made available through FDP. When we do, the 'last edited' date on this page will also change. Any changes to this notice will apply immediately from the date of any change.

NHS England merger with NHS Digital and Health Education England

Information about our organisations' merger and links to privacy information

In November 2021 the then Secretary of State for Health and Social Care set out their intention to merge Health Education England with NHS England, and also accepted a recommendation from the Chair of NHS Digital to merge NHS Digital with NHS England.

The expected date for NHS Digital to merge with NHS England is the 1 February 2023, and the expected date for Health Education England to merge with the new NHS England is the 1 April.

For data protection purposes, from 1st February 2023 NHS England will become the controller responsible for the processing of personal data for activities performed by NHS Digital prior to this date. Similarly, from 1 April 2023 NHS England will become the controller responsible for the processing of personal data for activities performed by Health Education England prior to this date.

As part of this merger the organisation will be undergoing a transitionary process, and within that transition the organisation will be operating dual privacy notices to provide information about the new NHS England's processing of personal data. From the respective merger dates, references to 'NHS Digital' and 'Health Education England' should be read as 'NHS England'.

The NHS Digital notice can be found here: Privacy and cookies - NHS England Digital. The Health Education England privacy notice can be found here: NHS England » Privacy and cookies. For subjects rights requests to your personal data you can contact either of the given contact details on the NHS England and NHS Digital privacy notices.

Artificial Intelligence Deployment Platform Pilot

How we use personal data to evaluate the effectiveness of a centralised hub to provide AI diagnostic support for radiological imaging in Trusts

AI Deployment Platform Pilot

Purposes for processing

NHS England and the Department of Health and Social Care (DHSC) are implementing a pilot NHS Artificial Intelligence Deployment Platform (AIDP) for medical imaging diagnostic technologies.

The AIDP will provide a hub to receive radiological images submitted by Trusts, route them for diagnostic interpretation by an appropriate AI product, and (in live mode – see below) return them to Trusts with marked-up diagnoses for onward transfer to local systems. Radiologists will then be able to view images with AI generated diagnoses, which they can use to inform their diagnoses.

The programme goals are to test whether having a centralised platform and deployment processes:

1. Accelerates the safe and ethical deployment of trusted AI products (class IIa and class IIb) at multiple hospital sites.
2. Provides a cost and time-effective standard deployment process of AI products for NHS organisations and AI innovators
3. Provides reasonable access to post-market surveillance resources of AI vendors
4. Provides the case study for accelerating the broader adoption of technologies across NHS organisations.

To test this approach, several mature AI products from leading vendors will be deployed into the two Trust Imaging Networks initially in shadow (test) mode, before being potentially switched on live if deemed appropriate.

The AIDP programme is working with Trusts in East Midlands Radiology Consortium (EMRAD) and Thames Valley Radiology Network (TVRN) to facilitate the pilot.

How NHS England/DHSC uses personal data to provide AI diagnostics and for evaluation

Trusts will submit radiological images from their local systems to the AIDP. The AIDP will forward them to the AI diagnostic product appropriate to the type of image – disease, area of the body, type of image (X-ray, MRI). The AI product will then return diagnostically interpreted images to the AIDP.

This process will initially facilitate shadow mode testing, which may involve the comparison of diagnoses made by radiologists (also submitted to the AIDP) with AI generated diagnoses. In shadow mode, results will not be returned to Trusts for clinical decision making. The purpose here is to test the pathway and verify the operation of AI products as accessed by the Trust.

Subject to performance checks in shadow mode, a decision will be made in collaboration with the Trusts to move to live mode, in which the results will be returned to Trusts and transferred to hospital systems so they can be used by radiologists to support their clinical diagnoses.

Patient and imaging attributes will be analysed on the AIDP for the purposes of post-market surveillance – for presentation in user dashboards and for model validation reporting. This will include analysing by gender, weight and size, locality of residence, smoking status and ethnic group.

Images and associated data submitted by Trusts will be pseudomymised before they are uploaded to the AIDP. In live mode the results will be re-identified by the Trust when they are returned from the AIDP. Trusts will use a dedicated router to pseudonymise, transfer and re-identify the data.

Organisations and their roles

NHS England and DHSC will be responsible as joint controllers for the processing to deliver the AIDP.

Faculty Science Ltd. will act as a processor for the delivery of the AIDP and will instruct the following as sub-processors:

- Cimar – for the provision of the core AI Deployment Platform, as well as maintenance and support
- Royal Surrey NHS Foundation Trust (RSNFT) – for the development of the post market surveillance system
- AI product vendors. For the provision of AI diagnostic services in support of the following disciplines:
    - Lucida Medical Ltd. – for AI diagnostic interpretation of prostate MRI scans
    - Lunit Inc. (implementing Radiobotics ApS) – for AI diagnostic interpretation of musculo-skeletal x-rays
    - Lunit Inc. – for AI diagnostic interpretation of chest x-rays
    -

Trusts will be responsible as controllers for processing to extract data from local radiology systems, to pseudonymise and submit images with associated data to the AIDP, and in live

mode to receive and re-identify images with marked up diagnoses and associated data. RSNFT acts as a processor to provide and support the pseudonymisation and re-identification router that transfers data to and from the AIDP.

AI diagnostic products – procurement and assurance

AI products have been selected by a DHSC / NHS England-led tender process for the three disciplines.

As part of their tender submission, prospective AI vendors must complete the Digital Technology Assessment Criteria (DTAC). This includes compulsory requirements on clinical safety, data protection, technical security and interoperability. Bidders must pass all of these requirements to be considered further.

In order to be eligible for procurement, AI products must be approved class IIa or class IIb medical devices and CE/UKCA marked. AI product vendors can only place a UKCA mark on their product and place it on the market when they have received a certificate from the Approved Body. This means that AI products must conform with the relevant requirements in the Medical Devices Regulations 2002.

The procurement evaluation process requires bidders to respond to extensive questions that are assessed and given an evaluation score. These include questions on how the AI product was developed and trained, ensuring fairness and an ethical approach, risks of bias and how the algorithm's fairness is tested over time.

Categories of personal data

The data processed on the AIDP and by AI vendors' diagnostic products will be pseudonymised radiological images including x-rays, CT and MRI scans.

As the personal data processed on the AIDP and by connecting AI products will be pseudonymised by submitting Trusts, it will be anonymous to NHS England, DHSC and their processor / sub-processors.

Data fields that directly identify individuals will be converted to pseudonyms which can only be reversed by Trusts. Many fields other than direct identifiers are cleared or modified to reinforce anonymity.

Data fields that are retained for post-market surveillance purposes include gender, patient weight and size, locality of residence, smoking status and ethnic group.

Special Categories of Personal Data include health data and racial or ethnic origin.

Retention period

Pseudonymised images and results from the AI data will have a fixed retention period. Initially this will be no more than 30 days, though this may be subject to change depending on how the pilot scope evolves.

The following meta data related to studies will be retained for the duration of the pilot to monitor and validate the AI models as well as support post market surveillance activity:

- Ground truth results – i.e. the radiologist verdict or patient outcome for each pseudonymised study
- AI output results – i.e. a description of what the AI detected on the image and the location on the image
- Aggregated AI product performance data e.g. sensitivity, specificity, recall rate etc.
- Aggregated study processing data e.g. number of studies processed / failed / excluded etc.

Legal basis for processing

For UK GDPR purposes NHS England's lawful basis for processing is Article 6(1)(e) – '…exercise of official authority…'

For the processing of special categories data the bases are:

For health data

9(2)(h) – '…health or social care…' – for the provision of the testing service

For racial or ethnic origin

9(2)(b) – '…necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law…'