Practice privacy notice

As a registered patient, Stalbans surgery has a legal duty to explain how we use any personal information we collect about you at the organisation. We collect records about your health and the treatment you receive in both electronic and paper format.

Why do we have to provide this privacy notice?

We are required to provide you with this privacy notice by law. It provides information about how we use the personal and healthcare information we collect, store and hold about you. If you have any questions about this privacy notice or are unclear about how we process or use your personal information or have any other issue regarding your personal and healthcare information, then please contact our Data Protection Officer Nick Murphy

The main things the law says we must tell you about what we do with your personal data are:

- We must let you know why we collect personal and healthcare information about you
- We must let you know how we use any personal and/or healthcare information we hold about you
- We need to inform you in respect of what we do with it
- We need to tell you about who we share it with or pass it on to and why
- We need to let you know how long we can keep it for

What is a privacy notice?

A privacy notice (or 'fair processing notice') explains the information we collect about our patients and how it is used. Being open and providing clear information to patients about how an organisation uses their personal data is an essential requirement of the new UK General Data Protection Regulations (UK GDPR).

Under the UK GDPR, we must process personal data in a fair and lawful manner. This applies to everything that is done with patient's personal information. This means that the organisation must:

- Have lawful and appropriate reasons for the use or collection of personal data
- Not use the data in a way that may cause harm to the individuals (e.g., improper sharing of their information with third parties)
- Be open about how the data will be used and provide appropriate privacy notices when collecting personal data
- Handle personal data in line with the appropriate legislation and guidance

- Not use the collected data inappropriately or unlawfully

What is fair processing?

Personal data must be processed in a fair manner – the UK GDPR says that information should be treated as being obtained fairly if it is provided by a person who is legally authorised or required to provide it. Fair processing means that the organisation has to be clear and open with people about how their information is used.

Stalbans surgery manages patient information in accordance with existing laws and with guidance from organisations that govern the provision of healthcare in England such as the Department of Health and the General Medical Council.

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- UK General Data Protection Regulations 2016
- Data Protection Act 2018
- Human Rights Act 1998
- Common Law Duty of Confidentiality
- Health and Social Care Act 2012
- NHS Codes of Confidentiality and Information Security
- Information: To Share or Not to Share Review

This means ensuring that your personal confidential data (PCD) is handled clearly and transparently and in a reasonably expected way.

The Health and Social Care Act 2012 changed the way that personal confidential data is processed so it is important that our patients are aware of and understand these changes and that you have an opportunity to object and know how to do so.

The healthcare professionals who provide you with care maintain records about your health and any NHS treatment or care you have received (e.g., NHS Hospital Trust, GP surgery, walk-in clinic, etc.). These records help to provide you with the best possible healthcare.

NHS health records may be processed electronically, on paper or a mixture of both and we use a combination of working practices and technology to ensure that your information is kept confidential and secure.

Who is the data controller?

Stalbans surgery is registered as a data controller under the Data Protection Act 2018. Our registration can be viewed online in the public register at www.ico.gov.uk. This means we are responsible for handling your personal and healthcare information and collecting and storing it appropriately when you are seen by us as a patient.

We may also process your information for a particular purpose and therefore we may also be data processors. The purposes for which we use your information are set out in this privacy notice.

What type of information do we collect about you?

Information held by this organisation may include the following:

- Your contact details (such as your name, address and email address)
- Details and contact numbers of your next of kin
- Your age range, gender, ethnicity
- Details in relation to your medical history
- The reason for your visit to the organisation
- Any contact the organisation and/or your practice has had with you including appointments (emergency or scheduled), clinic visits, etc.
- Notes and reports about your health, details of diagnosis and consultations with our GPs and other health professionals within the healthcare environment involved in your direct healthcare
- Details about the treatment and care received
- Results of investigations such as laboratory tests, x-rays, etc.
- Relevant information from other health professionals, relatives or those who care for you
- Recordings of telephone conversations between yourself and the organisation

Information collected about you from others

We collect and hold data for the purpose of providing healthcare services to our patients and we will ensure that the information is kept confidential. However, we can disclose personal information if:

- It is required by law
- You provide your consent – either implicitly for the sake of your own care or explicitly for other purposes
- It is justified to be in the public interest

To ensure you receive the best possible care, your records are used to enable the care you receive. Information held about you may be used to help protect the health of the public and to help us to manage the NHS.

Information may be used for clinical audit purposes to monitor the quality of services provided, may be held centrally and may be used for statistical purposes. Where we do this, we ensure that patient records cannot be identified. Sometimes your information may be requested to be used for clinical research purposes – the organisation will always endeavour to gain your consent before releasing the information.

Improvements in information technology are also making it possible for us to share data with other healthcare providers with the objective of providing you with better care. You can choose to withdraw your consent to your data being used in this way. When the organisation is about to participate in any new data-sharing scheme, we will make patients aware by displaying prominent notices and on our website at least four weeks before the scheme is due to start. We will also explain clearly what you have to do to 'opt-out' of each new scheme.

A patient can object to their personal information being shared with other healthcare providers but if this limits the treatment that you can receive then the doctor will explain this to you at the time.

What is special category data?

The law states that personal information about your health falls into a special category of information because it is extremely sensitive. Reasons that may entitle us to use and process your information may be as follows:

Public interest	Where we may need to handle your personal information when it is considered to be in the public interest. For example, when there is an outbreak of a specific disease and we need to contact you for treatment or we need to pass your information to relevant organisations to ensure you receive advice and/or treatment
Consent	When you have given us consent
Vital interest	If you are incapable of giving consent and we have to use your information to protect your vital interests (e.g., if you have had an accident and you need emergency treatment)
Defending a claim	If we need your information to defend a legal claim against us by you or by another party

Providing you with medical care	Where we need your information to provide you with medical and healthcare services

The legal justification for collecting and using your information

The law says we need a legal basis to handle your personal and healthcare information.

Contract	We have a contract to deliver healthcare services to you. This contract provides that we are under a legal obligation to ensure that we deliver medical and healthcare services to the public.
Consent	Sometimes we also rely on the fact that you give us consent to use your personal and healthcare information so that we can take care of your healthcare needs. Please note that you have the right to withdraw consent at any time if you no longer wish to receive services from us.
Necessary care	Providing you with the appropriate healthcare where necessary The law refers to this as 'protecting your vital interests' where you may be in a position not to be able to consent.
Law	Sometimes the law obliges us to provide your information to an organisation

How do we use your information?

Your data is collected for the purpose of providing direct patient care; however, we are able to disclose this information if it is required by law, if you give consent or if it is justified in the public interest.

In order to comply with its legal obligations, this organisation may have to send data to NHS Digital when directed by the Secretary of State for Health under the Health and Social Care Act 2012. Additionally, we may have to contribute to national clinical audits and will send the data that is required by NHS Digital as the law allows. This may include demographic data, such as date of birth, and information about your health which is recorded in coded form; for example, the clinical code for diabetes or high blood pressure.

Under the General Data Protection Regulation, we will be lawfully using your information in accordance with:

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

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

Who can we provide your personal information to and why?

Whenever you use a health or care service, such as attending the local hospital or using the district nursing service, clinical information about you is collected to help ensure you get the best possible care and treatment. This information may be passed to other approved organisations where there is a legal basis to do so, to help with planning services, improving care, researching to develop new treatments and preventing illness. All of this helps in providing better care to you and your family and future generations.

However, as explained in this privacy notice, confidential information about your health and care is only used in this way as allowed by law and would never be used for any other purpose without your clear and explicit consent.

We may pass your personal information on to the following people or organisations because these organisations may require your information to assist them in the provision of your direct healthcare needs. It therefore may be important for them to be able to access your information in order to ensure they may deliver their services to you:

- Hospital professionals (such as doctors, consultants, nurses etc.)
- Other GPs/doctors
- Primary Care Networks
- NHS Trusts/Foundation Trusts/Specialist Trusts
- NHS Commissioning Support Units
- NHS England (NHSE) and NHS Digital (NHSD)
- Multi-agency Safeguarding Hub (MASH)

- Independent contractors such as dentists, opticians, pharmacists
- Any other person who is involved in providing services related to your general healthcare including mental health professionals
- Private sector providers including pharmaceutical companies to allow for the provision of medical equipment, dressings, hosiery etc.
- Voluntary sector providers
- Ambulance Trusts
- Integrated Care Systems
- Clinical Commissioning Groups
- Local authority
- Social care services
- Education services
- Other 'data processors', e.g., Diabetes UK

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

Who may we provide your information to:

- For the purposes of complying with the law, e.g., the police

- Anyone you have given your consent to, to view or receive your record, or part of your record. If you give another person or organisation consent to access your record, we will need to contact you to verify your consent before we release that record. It is important that you are clear and understand how much and what aspects of your record you give consent to be disclosed

- Computer systems – we operate a clinical computer system on which NHS staff record information securely. This information can then be shared with other clinicians so that everyone caring for you is fully informed about your medical history including allergies and medication. We will make information available to our partner organisations (above) unless you have declined data sharing to ensure you receive appropriate and safe care. Wherever possible, staff will ask your consent before your information is viewed.

- Extended access – we provide extended access services to our patients so that you can access medical services outside of our normal working hours. To provide you with this service, we have formal arrangements in place with the Clinical Commissioning Group whereby certain key 'hubs' offer this service for you as a patient to access outside of our opening hours.

  This means those key 'hubs' will have to have access to your medical record to be able to offer you the service. Please note to ensure that those hubs comply with the law and to protect the use of your information, we have very robust data sharing agreements and other clear arrangements in place to ensure your data is always protected and used for those purposes only

Data extraction by the Clinical Commissioning Group – the Clinical Commissioning Group at times extracts medical information about you but the information we pass to them via our computer systems cannot identify you to them

This information only refers to you by way of a code that only your own practice can identify (it is pseudo-anonymised). This therefore protects you from anyone who may have access to this information at the Clinical Commissioning Group from ever identifying you as a result of seeing the medical information and we will never give them the information that would enable them to do this

Your rights as a patient

The law gives you certain rights to your personal and healthcare information that we hold as set out below:

Access and Subject Access Requests	You have a right under the Data Protection legislation to request access to view or to obtain copies of what information the organisation holds about you and to have it amended should it be inaccurate. To request this, you need to do the following: ○ Your request should be made to Stalbans Surgery ○ For information from a hospital or other Trust/NHS organisation you should write directly to them ○ There is no charge to have a copy of the information held about you. However, we may, in some limited and exceptional circumstances, have to make an administrative charge for any extra copies if the information requested is excessive, complex or repetitive ○ We are required to provide you with information within one month. We would ask therefore that any requests you make are in writing and it is made clear to us what and how much information you require ○ You will need to give adequate information (for example full name, address, date of birth, NHS number and details of your request) so that your identity can be verified and your records located
Correction	We want to make sure that your personal information is accurate and up to date.

	You may ask us to correct any information you think is inaccurate. It is especially important that you make sure you tell us if your contact details including your mobile phone number have changed
Removal	You have the right to ask for your information to be removed. However, if we require this information to assist us in providing you with appropriate medical services and diagnosis for your healthcare, then removal may not be possible
Objection	We cannot share your information with anyone else for a purpose that is not directly related to your health, e.g., medical research, educational purposes etc.
Transfer	You have the right to request that your personal and/or healthcare information is transferred, in an electronic form (or other form), to another organisation but we will require your clear consent to be able to do this.

How long do we keep your personal information?

We are required under UK law to keep your information and data for the full retention periods as specified by the NHS Records Management Code of Practice for health and social care and national archives requirements.

More information on records retention can be found online at: NHSX – Records Management Code of Practice 2021.

Where do we store your information electronically?

All the personal data we process is processed by our staff in the UK. However, for the purposes of IT hosting and maintenance this information may be located on servers within the European Union.

No third parties have access to your personal data unless the law allows them to do so and appropriate safeguards have been put in place such as a data processor as above. We have data protection processes in place to oversee the effective and secure processing of your personal and/or special category data.

Stalbans surgery uses a clinical system provided by a data processor called EMIS. With effect from 10 June 2019, EMIS started storing the organisation's EMIS web data in a highly secure, third-party cloud hosted environment, namely Amazon Web Services ('AWS').

Data does remain in the UK and will be fully encrypted both in transit and at rest. In doing this, there will be no change to the control of access to your data and the hosted service provider will not have any access to the decryption keys. AWS is one of the world's largest cloud companies, already supporting numerous public sector clients (including the NHS), and it offers the highest levels of security and support.

Maintaining your confidentiality and accessing your records

We are committed to protecting your privacy and will only use information collected lawfully in accordance with the UK General Data Protection Regulations (which is overseen by the Information Commissioner's Office), Human Rights Act, the Common Law Duty of Confidentiality and the NHS Codes of Confidentiality and Security. Every staff member who works for an NHS organisation has a legal obligation to maintain the confidentiality of patient information.

All of our staff, contractors and locums receive appropriate and regular training to ensure they are aware of their personal responsibilities and have legal and contractual obligations to uphold confidentiality, enforceable through disciplinary procedures. Only a limited number of authorised staff have access to personal information where it is appropriate to their role and this is strictly on a need-to-know basis. If a sub-contractor acts as a data processor for Stalbans surgery, an appropriate contract (Article 24-28) will be established for the processing of your information.

We maintain our duty of confidentiality to you at all times. We will only ever use or pass on information about you if others involved in your care have a genuine need for it. We will not disclose your information to any third party without your permission unless there are exceptional circumstances (i.e., life or death situations) or where the law requires information to be passed on and/or in accordance with the information sharing principle following Dame Fiona Caldicott's information sharing review (Information to share or not to share) where "The duty to share information can be as important as the duty to protect patient confidentiality." This means that health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by the Caldicott principles.

Our organisational policy is to respect the privacy of our patients, their families and our staff and to maintain compliance with the UK General Data Protection Regulation (UK GDPR) and all UK specific data protection requirements. Our policy is to ensure all personal data related to our patients will be protected.
In certain circumstances you may have the right to withdraw your consent to the processing of data. Please contact the organisation in writing if you wish to withdraw your consent. In some circumstances we may need to store your data after your consent has been withdrawn to comply with a legislative requirement.

Sharing your information without consent

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

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

Third party processors

To enable us to deliver the best possible services, we will share data (where required) with other NHS bodies such as hospitals. In addition, the organisation will use carefully selected third party service providers. When we use a third-party service provider to process data on our behalf then we will always have an appropriate agreement in place to ensure that they keep the data secure, that they do not use or share information other than in accordance with our instructions and that they are operating appropriately. Examples of functions that may be carried out by third parties include:

- Companies that provide IT services and support, including our core clinical systems, systems that manage patient facing services (such as our website and service accessible through the same), data hosting service providers, systems that facilitate appointment bookings or electronic prescription services and document management services etc.

- Further details regarding specific third-party processors can be supplied on request to the data protection officer as below.

Third parties mentioned on your medical record

Sometimes we record information about third parties mentioned by you to us during any consultation. We are under an obligation to make sure we also protect that third party's rights as an individual and to ensure that references to them that may breach their rights to confidentiality are removed before we send any information to any other party including yourself. Third parties can include spouses, partners and other family members.

Anonymised information

Sometimes we may provide information about you in an anonymised form. If we do so, then none of the information we provide to any other party will identify you as an individual and cannot be traced back to you.

Audit

Auditing of clinical notes is done by Stalbans surgery as part of their commitment to the effective management of healthcare whilst acting as a data processor.

Article 9.2.h is applicable to the management of healthcare services and “permits processing necessary for the purposes of medical diagnosis, provision of healthcare and treatment, provision of social care and the management of healthcare systems or services or social care systems or services.’” No consent is required to audit clinical notes for this purpose.

Furthermore, compliance with Article 9(2)(h) requires that certain safeguards are met. The processing must be undertaken by or under the responsibility of a professional subject to the obligation of professional secrecy or by another person who is subject to an obligation of secrecy.

Auditing clinical management is no different to a multi-disciplinary team meeting discussion whereby management is reviewed and agreed. It would be realistically impossible to require consent for every patient reviewed that is unnecessary. It is also prudent to audit under Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17: Good Governance.

Computer System

This organisation operates a clinical computer system on which NHS staff record information securely. This information can then be shared with other clinicians so that everyone caring for you is fully informed about your medical history including allergies and medication.

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

GP connect service

We use a facility called GP Connect to support your direct care. GP Connect makes patient information available to all appropriate clinicians when and where they need it, to support direct patient care, leading to improvements in both care and outcomes. GP Connect is not used for any purpose other than direct care.

Authorised clinicians such as GPs, NHS 111 clinicians, care home nurses (if you are in a care home), secondary care trusts and social care clinicians are able to access the GP records of the patients they are treating via GP connect.

The NHS 111 service (and other services determined locally e.g., other GP practices in a Primary Care Network) will be able to book appointments for patients at GP practices and other local services.

Invoice validation

Your information may be shared if you have received treatment to determine which Clinical Commissioning Group (CCG) is responsible for paying for your treatment. This information may include your name, address and treatment date. All of this information is held securely and confidentially; it will not be used for any other purpose or shared with any third parties.

NHS health checks

Cohorts of our patients aged 40-74 not previously diagnosed with cardiovascular disease are eligible to be invited for an NHS Health Check. Nobody outside the healthcare team in Stalbans surgery will see confidential information about you during the invitation process.

Patient communication

As we are obliged to protect any confidential information we hold about you, it is imperative that you let us know immediately if you change any of your contact details.

We may contact you using SMS texting to your mobile phone should we need to notify you about appointments and other services that we provide to you involving your direct care. This is to ensure we are sure we are contacting you and not another person. As this is operated on an 'opt out' basis we will assume that you have given us permission to contact you via SMS if you have provided your mobile telephone number. Please let the organisation know if you wish to opt out of this SMS service. We may also contact you using the email address you have provided to us.

Primary care networks

The objective of primary care networks (PCNs) is for group practices together to create more collaborative workforces that ease the pressure of GPs, leaving them better able to focus on patient care. All areas within England are covered by a PCN.

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

All GP practices have come together in geographical networks covering populations of approximately 30–50,000 patients to take advantage of additional funding attached to the GP contract. This size is consistent with the size of the primary care homes that exist in many places in the country but are much smaller than most GP federations.

This means that Stalbans surgery may share your information with other practices within the Primary Care Network to provide you with your care and treatment.

Risk stratification

Risk stratification is a mechanism used to identify and subsequently manage those patients deemed as being at high risk of requiring urgent or emergency care. Usually this includes patients with long-term conditions, e.g., cancer. Your information is collected by a number of sources including Stalbans surgery. This information is processed electronically and given a risk score which is relayed to your GP who can then decide on any necessary actions to ensure that you receive the most appropriate care.

Safeguarding

The organisation is dedicated to ensuring that the principles and duties of safeguarding adults and children are consistently and conscientiously applied with the wellbeing of all at the heart of what we do.

Our legal basis for processing for UK General Data Protection Regulation (UK GDPR) purposes 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…'*

Safeguarding information such as referrals to safeguarding teams is retained by Stalbans surgery when handling a safeguarding concern or incident. We may share information accordingly to ensure a duty of care and investigation as required with other partners such as local authorities, the police or healthcare professionals (i.e., the mental health team).

Shared care

To support your care and improve the sharing of relevant information to our partner organisations (as above) when they are involved in looking after you, we will share information to other systems.

You can opt out of this sharing of your records with our partners at any time if this sharing is based on your consent.

Summary care records

During the height of the pandemic changes were made to the Summary Care Record (SCR) to make additional patient information available to all appropriate clinicians when and where they needed it to support direct patient care, leading to improvements in both care and outcomes.

These changes to the SCR will remain in place unless you decide otherwise.

Regardless of your past decisions about your SCR preferences, you will still have the same options that you currently have in place to opt out of having a SCR, including the opportunity to opt back in to having a SCR or opt back in to allow the sharing of additional information.

You can exercise these choices by doing the following:

- Choosing to have a SCR with all information shared. This means that any authorised, registered and regulated health and care professionals will be able to see a detailed SCR, including core and additional information if they need to provide you with direct care.

- Choosing to have a SCR with core information only. This means that any authorised, registered and regulated health and care professionals will be able to see limited information about allergies and medications in your SCR if they need to provide you with direct care.

- Choosing to opt-out of having a SCR altogether. This means that you do not want any information shared with other authorised, registered and regulated health and care professionals involved in your direct care. You will not be able to change this preference at the time if you require direct care away from your GP practice. This means that no authorised, registered and regulated health and care professionals will be able to see information held in your GP records if they need to provide you with direct care, including in an emergency.

To make these changes, you should inform your GP practice or complete this form and return it to your GP practice.

Organisation website

Our website does use cookies to optimise your experience. Using this feature means that you have agreed to the use of cookies as required by the EU Data Protection Directive 95/46/EC. You have the option to decline the use of cookies on your first visit to the website. The only website this privacy notice applies to is Stalbans surgery website.

If you use a link to any other website from the organisation's website then you will need to read their respective privacy notice. We take no responsibility (legal or otherwise) for the content of other websites.

Opt-outs

National opt-out facility

This is used by the NHS, local authorities, university and hospital researchers, medical colleges and pharmaceutical companies researching new treatments.

You can choose to opt out of sharing your confidential patient information for research and planning. There may still be times when your confidential patient information is used; for example, during an epidemic where there might be a risk to you or to other people's health. You can also still consent to take part in a specific research project.

Your confidential patient information will still be used for your individual care. Choosing to opt out will not affect your care and treatment. You will still be invited for screening services such as screening for bowel cancer.

You do not need to do anything if you are happy about how your confidential patient information is used.

If you do not want your confidential patient information to be used for research and planning, you can choose to opt out by using one of the following:

- **Online service** – patients registering need to know their NHS number or their postcode as registered at their GP practice

- **Telephone service** 0300 303 5678 which is open Monday to Friday between 0900 and 1700

- **NHS App** – for use by patients aged 13 and over (95% of surgeries are now connected to the NHS App). The app can be downloaded from the App Store or Google play

- "**Print and post"** registration form: https://assets.nhs.uk/prod/documents/Manage_your_choice_1.1.pdf

  Photocopies of proof of applicant's name (e.g., passport, UK driving licence etc.) and address (e.g., utility bill, payslip etc.) need to be sent with the application. It can take up to 14 days to process the form once it arrives at NHS, PO Box 884, Leeds, LS1 9TZ.

- Getting a healthcare professional to assist patients in prison or other secure settings to register an opt-out choice. For patients detained in such settings, guidance is available on NHS Digital and a proxy form is available to assist in registration.

Note: Unfortunately, the national data opt-out cannot be applied by this organisation.

General Practice Data for Planning and Research opt out (GPDPR)

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

- Monitor the long-term safety and effectiveness of car
- Plan how to deliver better health and care services
- Prevent the spread of infectious diseases
- Identify new treatments and medicines through health research

GP practices already share patient data for these purposes but this new data collection will be more efficient and effective. This means that GPs can get on with looking after their patients and NHS Digital can provide controlled access to patient data to the NHS and other organisations who need to use it, to improve health and care for everyone.

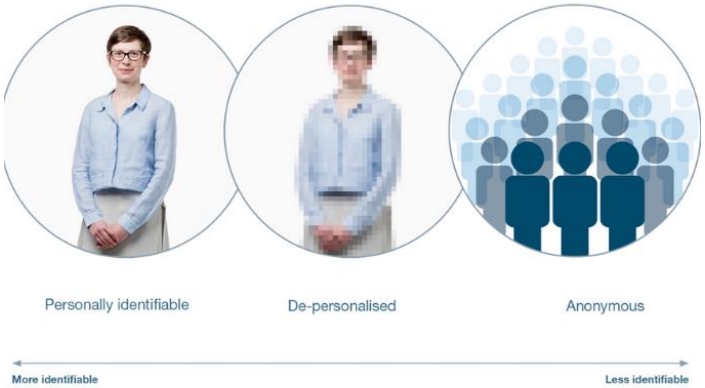
Contributing to research projects will benefit us all as better and safer treatments are introduced more quickly and effectively without compromising your privacy and confidentiality.

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

What patient data is shared about you with NHS Digital?

The collection date is still to be confirmed, although when it has been, patient data will be collected from GP medical records about:

- Any living patient registered at a GP practice in England when the collection started – this includes children and adults
- Any patient who died after the data collection started and was previously registered at a GP practice in England when the data collection started



They will not collect your name or where you live. Any other data that could directly identify you, for example NHS number, General Practice Local Patient Number, postcode and date of birth, is replaced with unique codes that are produced by de-identification software before the data is shared with NHS Digital.

This process is called pseudonymisation and means that no one will be able to directly identify you from the data. The diagram helps to explain what this means. The diagram below helps to explain what this means and using the terms in the diagram, the data we share would be described as de-personalised.

Image provided by Understanding Patient Data under licence.

The data collected by NHS Digital

We will share structured and coded data from GP medical records that is needed for specific health and social care purposes as explained above.

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

NHS Digital will collect:

- Data on your sex, ethnicity, and sexual orientation

- Clinical codes and data about diagnoses, symptoms, observations, test results, medications, allergies, immunisations, referrals and recalls and appointments including information about your physical, mental, and sexual health

- Data about the staff who have treated you

More detailed information about the patient data collected is contained within the Data Provision Noticed issued to GP practices.

NHS Digital will not collect:

- Your name and address (except for your postcode in unique coded form)
- Written notes (free text) such as the details of conversations with doctors and nurses
- Images, letters and documents
- Coded data that is not needed due to its age – for example medication, referral and appointment data that is over 10 years old
- Coded data that GPs are not permitted to share by law – for example certain codes about IVF treatment and certain information about gender re-assignment

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

When NHS Digital collects, analyses, publishes and shares patient data, there are strict laws in place that it must follow. Under the UK General Data Protection Regulation (UK GDPR), this includes explaining to patients what legal provisions apply under UK GDPR that allows it to process patient data. The UK GDPR protects everyone's data.

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

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

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

Regulation 3 of the Health Service (Control of Patient Information) Regulations 2002 (COPI) also allows confidential patient information to be used and shared appropriately and lawfully in a public health emergency. The Secretary of State has issued legal notices under COPI (COPI Notices) requiring NHS Digital, NHS England and Improvement, arm's-length bodies (such as Public Health England), local authorities, NHS trusts, clinical commissioning groups and GP practices to share confidential patient information to respond to the COVID-19 outbreak.

Any information used or shared during the COVID-19 outbreak will be limited to the period of the outbreak unless there is another legal basis to use confidential patient information.

How NHS Digital uses patient data

NHS Digital will analyse and link the patient data we collect with other patient data we hold to create national data sets and for data quality purposes. NHS Digital will be able to use the de-identification software to convert the unique codes back to data that could directly identify patients in certain circumstances for these purposes, where this is necessary and where there is a valid legal reason. There are strict internal approvals which need to be in place before NHS Digital can do this and this will be subject to independent scrutiny and oversight by the Independent Group Advising on the Release of Data (IGARD).

These national data sets are analysed and used by NHS Digital to produce national statistics and management information including public dashboards about health and social care which are published. NHS Digital never publish any patient data that could identify any individual. All data they publish is anonymous statistical data.

For more information about data NHS Digital publish see Data and Information and Data Dashboards.

Who does NHS Digital share patient data with?

All data that is shared by NHS Digital 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 be shared.

All requests to access patient data from this collection, other than anonymous aggregate statistical data, will be assessed by NHS Digital's Data Access Request Service to make sure that organisations have a legal basis to use the data and that it will be used safely, securely and appropriately.

These requests for access to patient data will also be subject to independent scrutiny and oversight by the Independent Group Advising on the Release of Data (IGARD). Organisations approved to use this data will be required to enter into a data sharing agreement with NHS Digital regulating the use of the data.

There are several organisations that are likely to need access to different elements of patient data from the General Practice Data for Planning and Research collection. These include but may not be limited to:

- The Department of Health and Social Care and its executive agencies including Public Health England and other government departments
- NHS England and NHS Improvement
- Primary care networks (PCNs), clinical commissioning groups (CCGs) and integrated care organisations (ICOs)
- Local authorities
- Research organisations including universities, charities, clinical research organisations that run clinical trials and pharmaceutical companies

If the request is approved, the data will either be made available within a secure data access environment within the NHS Digital infrastructure or, where the needs of the recipient cannot be met this way, as a direct dissemination of data. NHS Digital plan to reduce the amount of data being processed outside central, secure data environments and increase the data it makes available to be accessed via its secure data access environment.

Data will always be shared in the uniquely coded form (de-personalised data in the diagram above) unless in the circumstances of any specific request it is necessary for it to be provided in an identifiable form (personally identifiable data in the diagram above), for example, when express patient consent has been given to a researcher to link patient data from the General Practice for Planning and Research collection to data the researcher has already obtained from the patient. It is therefore possible for NHS Digital to convert the unique codes back to data that could directly identify patients in certain circumstances, and where there is a valid legal reason which permits this without breaching the common law duty of confidentiality. This would include:

- Where the data is needed by a health professional for the patient's own care and treatment
- Where the patient has expressly consented to this, for example to participate in a clinical trial
- Where there is a legal obligation, for example where there are COPI Notices

- Where approval has been provided by the Health Research Authority or the Secretary of State with support from the Confidentiality Advisory Group (CAG) under Regulation 5 of the Health Service (Control of Patient Information) Regulations 2002 (COPI) - this is sometimes known as a 'section 251 approval'

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

Details of who NHS Digital have shared data with, in what form and for what purposes are published on their data release register.

Where does NHS digital store patient data?

NHS Digital only stores and processes patient data for this data collection within the United Kingdom (UK). Fully anonymous data (that does not allow patients to be directly or indirectly identified), for example statistical data that is published, may be stored and processed outside of the UK.

Some of the NHS Digital processors may process patient data outside of the UK. If they do, they will always ensure that the transfer outside of the UK complies with data protection laws.

Changes to our privacy policy

We regularly review our privacy policy and any updates will be published on our website, in our newsletter and on posters to reflect the changes. This policy is to be reviewed yearly.