SOUTH & WEST HEREFORDSHIRE PRIMARY CARE NETWORK (PCN)

DATA PROTECTION PRIVACY NOTICE FOR PATIENTS

INTRODUCTION

As the South & West Herefordshire Primary Care Network (Alton Street Surgery, Fownhope Surgery, Golden Valley Surgery, Kingstone Surgery, Much Birch Surgery and Pendeen Surgery), we understand how important it is to keep your personal information safe and secure, and we take this very seriously. We have taken steps to make sure your personal information is looked after in the best possible way, and we review this regularly. We have robust policies and procedures in place including an Information Governance Policy. We have also adopted a 'privacy by design' approach and this helps to ensure that we consider the privacy implications of our systems and services.

Please read this Privacy Notice carefully as it contains important information about how we use your personal and healthcare information that you give to us, or any information that we may collect from you or about you from other organisations.

This Notice explains

- Who we are and how we use your information
- Information about our Data Protection Officer
- What kinds of personal information about you we hold and use (process)
- The legal grounds for our processing of your personal information (including when we share it with others)
- What should you do if your personal information changes?
- For how long your personal information is retained/stored by us?
- What are your rights under Data Protection laws

For the purpose of applicable data protection legislation (including, but not limited to, the General Data Protection Regulation (Regulation (UK) 2016/679) (the "UKGDPR"), and the Data Protection Act 2018 the organisation responsible for your personal data is your registered practice within the South & West Herefordshire Primary Care Network.

WHY ARE WE PROVIDING THIS PRIVACY NOTICE?

A Privacy Notice (or 'Fair Processing Notice') is an explanation of what information the organisation collects on patients, and how it is used. Being transparent and providing clear information to patients about how an organisation uses their personal data is an essential requirement of the UK General Data Protection Regulations (UK GDPR).

We are required to provide you with this Privacy Notice by law. We are bound by the UK GDPR which includes principles that we must apply when collecting and using your data. These are:

- To process your data in a manner which is lawful, fair and transparent. This means that when we collect and use your information, we must have a lawful basis for doing so, we must consider the rights and interests of the data we collect about you and provide clear information about our use of your data.

- Collecting your data for a specified and legitimate purposes and not used in any ways which are incompatible with those. When we collect your data, we must be very clear about why we need it and what we will do with it. If we do collect data for one purpose, then rightly, we may not use it for an unconnected purpose.

- Your data we collect must be adequate, relevant and limited to what is necessary for the purposes for which it is. This means we must make sure that we only collect and use data that is strictly necessary for our stated purpose or purposes.

- Data must be accurate, and where necessary, kept up to date. We are required to take all reasonable steps to ensure that the data held is correct and kept up to date. This means that from time to time, we will review the data we hold and may contact you to make sure the data we have about you is current.

- Data must be kept for no longer than is necessary for the purposes for which it is held. In some cases, it may only be necessary for us to be able to directly identify you for a short period of time.

- Data must be used in a manner that ensures appropriate security of the data. This means that our policies, procedures, systems and working practices must ensure your data is always kept secure.

FAIR PROCESSING

Personal data must be processed in a fair manner. Fair Processing means that the organisation must be clear and open with people about how their information is used.

We manage 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

In short, this means ensuring that your personal confidential data (PCD) is handled clearly and transparently, and in an expected way.

The Health and Social Care Act 2012 changed the way that personal confidential data is processed, therefore 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 health care 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 are used to ensure that your information is kept confidential and secure.

WHO IS THE DATA CONTROLLER?

Your registered practice and the PCN will be what is known as 'Joint Controllers' of your personal data under the Data Protection Act 2018. We will collect basic personal data about you and location-based information. This means we are responsible for collecting, storing and handling your personal and healthcare information when you are seen by us as a patient.

There may be times when we also process your information. That means we use it for a particular purpose and, therefore, on those occasions we may also be data processors.

INFORMATION WE COLLECT FROM YOU

The health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously. These records help to provide you with the best possible healthcare and treatment.

Records held by this organisation may include the following information:

- Your contact details (such as your name, address and email address including place of work and work contact details)
- 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
- Any contact the PCN 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 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 including clinical consultations, and these may be used for training, quality and dispute resolution purposes.

HOW DO WE LAWFULLY USE YOUR DATA?

We need your personal, sensitive and confidential data in order to provide you with healthcare services as a General Practice, 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

This Privacy Notice applies to the personal data of our patients and the data you have given us about your carers/family members.

We use your personal and healthcare information in the following ways:

- when we need to speak to, or contact other doctors, consultants, nurses or any other medical/healthcare professional or organisation during your diagnosis or treatment or on-going healthcare.

- when we are required by law to hand over your information to any other organisation, such as the police, by court order, solicitors, or immigration enforcement.

- In a de-identified form to support planning of health services and to improve health outcomes for our population

We will never pass on your personal information to anyone else who does not need it, or has no right to it, unless you give us consent to do so.

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 with NHS England 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 (see above).

SPECIAL CATEGORIES

The law states that personal information about your health falls into a special category of information because it is 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 must use your information to protect your vital interests (eg 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

PRIMARY CARE NETWORK

The objective of primary care networks (PCNs) is for group practices together to create more collaborative workforces which ease the pressure of GP's, leaving them better able to focus on patient care.

South & West Herefordshire PCN consists of the following practices:

- Kingstone Surgery
- Golden Valley Surgery
- Fownhope Medical Centre
- Alton Street Surgery
- Pendeen Surgery

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

This means your registered practice may share your information with other practices within the PCN to provide you with your care and treatment, including an extended access service outside of the normal working hours.

Please note to ensure that those practices comply with the law and to protect the use of your information, we have a very robust data sharing agreement and other clear arrangements in place to ensure your data is always protected and used for those purposes only.

WHO ARE OUR PARTNER ORGANISATIONS?

Whenever you use a health or care service, such as attending Accident and Emergency or using Community Care Services, important 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 help with planning services, improving care, research into developing 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 organisation 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 to ensure they may professionally deliver their services to you:

- NHS Trust, Foundation Trusts, Special Trust, Hospital professionals (such as doctors, consultants, nurses etc)
- Other GPs/Doctors
- Other professionals involved in providing your healthcare, for example mental health professionals, physiotherapists
- Child Health Immunisation Service (CHIS)
- NHS Commissioning Support units
- Primary Care Networks – case management system Joy
- Independent Contractors such as dentists, opticians, pharmacists
- Any other person that is involved in providing services related to your general healthcare, including mental health professionals
- Private Sector Providers including pharmaceutical companies to allow for provision of medical equipment, dressings, hosiery etc
- Voluntary Sector Providers such as Carers Support
- Ambulance Trusts
- Integrated Care Boards
- Community Health Services such as district nurses
- Local Authorities
- Social Care Services
- Education Services
- NHS England (NHSE) and NHS Digital (NHSD)
- Multi-Agency Safeguarding Hub (MASH)
- Fire and Rescue Services
- Police and Judicial Services
- IGPR, Lexacom (Aprobrium)
- Analyse Rx/Optimise Rx services which support safe, evidence-based, quality prescribing
- AccuRx text messaging service
- Other ‘data processors’ which you will be informed of

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.

OTHER PEOPLE WHO WE PROVIDE YOUR INFORMATION TO

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

- Anyone you have given your consent to, to view or receive your record, or part of your record – please note, 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.

- Herefordshire & Worcestershire Shared Care Record – Patients in Herefordshire can benefit from the sharing of information to better manage their care via the Shared Care Record system. This includes sharing: contact details, diagnosis, medications, allergies, test results, referral and letters and care plans between health professionals

  Being able to see this information will help them give you the best care as quickly as possible without having to make phone calls or wait for other organisations to forward details on. Some of their administrative and secretarial staff will also be able to see information so they can support the professionals. An example would be to send you an appointment letter.

  All staff must follow the law on keeping your information confidential. Each time they look at your records this will be recorded to make sure they are only looking at the right information, for the right reasons.

  Health information is shared with:

  - GP practices in Herefordshire and Worcestershire
  - Worcestershire Acute Hospitals NHS Trust
  - Wye Valley NHS Trust
  - Herefordshire and Worcestershire Health and Care NHS Trust
  - West Midlands Ambulance Service University NHS Foundation Trust
  - Worcestershire County Council
  - Herefordshire Council
  - St Richards Hospice
  - Primrose Hospice
  - Kemp Hospice
  - St Michael's Hospice

  Further information about the Shared Record can be found be going to the following web page:

  Herefordshire & Worcestershire Shared Care Record

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.

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 a Data Protection regime in place to oversee the effective and secure processing of your personal and or special category (sensitive, confidential) data.

The PCN operates a clinical computer system called EMIS 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.

From 10th June 2019, EMIS, as data processor, started storing this organisation's EMIS Web data in a highly secure, third-party cloud hosted environment, namely Amazon Web Services ("AWS").

This data will always 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 very highest levels of security and support.

HOW LONG WILL WE STORE YOUR 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 (Records Management Code of Practice 2023).

HOW DO WE MAINTAIN THE CONFIDENTIALITY OF YOUR RECORDS?

Every staff member who works for an NHS organisation has a legal obligation to maintain the confidentiality of patient information.

All 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 is strictly on a need-to-know basis.

We always maintain our duty of confidentiality to you. 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), 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 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.

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

In certain circumstances you may have the right to withdraw your consent to the processing of data. Please contact the Reception Team of your registered practice 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.

INTERNATIONAL TRANSFERS OF YOUR PERSONAL DATA

Under the UK General Data Protection Regulation and other data protection law, information about you may only be transferred from your region to other regions if certain requirements are met.

While providing our services, occasionally we may need to transfer your data to doctors working in countries outside of the jurisdiction in which you reside. These countries may have data protection laws that differ from those in your country of residence. You should be assured that we will take all necessary steps to ensure that your personal data is adequately protected as required by applicable data protection laws.

The transfer of your personal data outside of your country of residence may be necessary for a consultation to take place between you and a clinician. Additionally, your explicit consent may serve as the legal basis for certain data transfers.

When transferring your personal data internationally, we will employ appropriate safeguards to ensure its security and protection. Such safeguards may include:

a. ***Standard Contractual Clauses***: We may use contractual agreements approved by relevant data protection authorities to ensure that your personal data receives the same level of protection as required in your country of residence.

b. ***Adequacy Decisions***: If the European Commission or other relevant data protection authorities have determined that a specific country ensures an adequate level of data protection, we may rely on such decisions for the transfer of personal data to that country. These counties include Andorra, Argentina, Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Faroe Islands, Finland, France, Germany, Gibraltar, Greece, Guernsey, Hungary, Iceland, Ireland, Isle of Man, Israel, Italy, Japan, Jersey, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and Uruguay.

Appropriate data transfer risk assessments and international data transfer assessments will be undertaken as required to meet appropriate legislative requirements. The PCN also confirms that the clinicians we retain to provide our services are required to adhere to our Privacy Policy and principles as well as all applicable local Data Protection laws and regulations.

GP CONNECT SERVICE AND DATA SHARING

We use a facility called GP Connect to support your direct care. This interface programme makes patient information available to all appropriate clinicians when and where they need it, to support direct patients 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, Social Care Clinicians are able to access the GP records of the patients they are treating via a secure NHS Digital service called GP connect.

The NHS 111 service (and other services) will be able to book appointments for patients at GP practices and other local services.

Explicit consent is not required when information is shared for a direct care purpose. If a patient does not want their information to be shared using GP Connect, they can opt out

Further details about GP Connect are available here: GP Connect privacy notice - NHS Digital.

THIRD PARTY PROCESSORS

To deliver the best possible service, the PCN will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition, the PCN 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 & support, including our core clinical systems; systems which manage patient facing services (such as our websites and service accessible through the same); data hosting service providers; systems which facilitate appointment bookings or electronic prescription services; document management services etc.

- Delivery services (for example if we were to arrange for delivery of any medicines to you).

- Payment providers (if for example you were paying for a prescription or a service such as travel vaccinations).

Further details regarding specific third-party processors can be supplied on request.

ANONYMISED INFORMATION

Sometimes we may provide information about you in an anonymised form. Such information is used to analyse population-level heath issues and helps the NHS to plan better services. If we share information for these purposes, then none of the information will identify you as an individual and cannot be traced back to you.

THIRD PARTIES MENTIONED ON YOUR MEDICAL RECORD

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

RISK STRATIFICATION

Risk stratification data tools are increasingly being used in the NHS to help determine a person's risk of suffering a condition, preventing an unplanned or (re)admission and identifying a need for preventive intervention. Information about you is collected from several sources including NHS Trusts and from this organisation. The identifying parts of your data are removed, analysis of your data is undertaken, and a risk score is then determined. This is then provided back to your GP as data controller in an identifiable form. Risk stratification enables your GP to focus on preventing ill health and not just the treatment of sickness.

If necessary, your GP may be able to offer you additional services. Please note that you have the right to opt out of your data being used in this way in most circumstances, please contact your registered practice for further information about opt out.

Individual Risk Management at a GP practice level however is deemed to be part of your individual healthcare and is covered by our legal powers above.

BRAVE AI

All practices in the PCN are committed to protecting your privacy and ensuring the confidentiality of your information.

We want to provide you with insight into how BRAVE AI is utilised across Primary Care Networks in the South & West Herefordshire area and its potential impact on your healthcare. BRAVE AI serves as a clinical decision support tool, empowering clinicians to make well-informed decisions about individualised care plans. It's essential to understand that the tool itself does not autonomously make decisions regarding interventions; instead, it assists healthcare professionals in their decision-making process.

BRAVE AI employs sophisticated computer algorithms to evaluate the complexity of each patient's health needs within our practice. By assigning a score, it helps identify individuals at risk of deteriorating health, potentially necessitating hospitalisation. This innovative tool enhances our ability to recognise patients who may otherwise be overlooked, including those with borderline health indicators or infrequent medical interactions.

It's crucial to emphasise that BRAVE AI does not utilise identifiable patient data. However, the provision of NHS numbers enables our PCN to pinpoint individual patients who may benefit from interventions. Furthermore, all data processed by BRAVE AI is stored securely within NHS network servers, inaccessible from external sources. Confidential patient information is exclusively disclosed to clinical teams directly involved in patient care.

The primary objective of BRAVE AI is to promote preventive healthcare practices over reactive treatments. It facilitates proactive discussions with patients regarding their overall wellbeing, extending beyond mere medical concerns. These conversations may involve various healthcare professionals, including Health Coaches and nurses, in addition to GPs.

Should you have any questions or concerns regarding the processing of your data alongside BRAVE AI, do please raise this with our Reception Team in the first instance.

AUDIT

Auditing of clinical notes is done by the PCN as part of our commitment to effective management of healthcare whilst acting as data controller.

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 be 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 which is unnecessary.

It is also prudent to audit under Health and Social Care Act 2008 (Regulated Activities) Regulations 2014: Regulation 17: Good Governance

MEDICINES MANAGEMENT

The PCN may conduct Medicines Management Reviews of medications prescribed to its patients. This service performs a review of prescribed medications to ensure patients receive the most appropriate, up to date and cost-effective treatments. The reviews are carried out by the ICBs Medicines Management Team under a Data Processing contract with your registered practice.

TRANSFERRING THE CURRENT PAPER MEDICAL RECORDS INTO PATIENTS' ELECTRONIC MEDICAL RECORDS

The following provisions of the UK General Data Protection Regulation permit us to digitise existing paper medical records:

- *Article 6(1)(e) – 'processing is necessary…in the exercise of official authority vested in the controller…''*

- *Article 9(2)(h) – 'processing is necessary for the purpose of preventative…medicine…the provision of health or social care or treatment or the management of health or social care systems and services…'*

The paper patient records will be shared with a scanning provider, who will scan and digitise the current paper medical records before destroying them. The paper patient records will be shared with the scanning provider above, who will scan and digitise the current paper medical records before destroying them.

OpenSAFELY COVID-19 SERVICE

NHS England has been directed by the Government to establish and operate the OpenSAFELY service. This service provides a Trusted Research Environment that supports COVID-19 research and analysis.

Each GP practice remains the controller of its own patient data but is required to let researchers run queries on pseudonymised patient data. This means identifiers are removed and replaced with a pseudonym, through OpenSAFELY.

Only researchers approved by NHS England are allowed to run these queries and they will not be able to access information that directly or indirectly identifies individuals. More information about OpenSAFELY can be found here: The NHS England OpenSAFELY COVID-19 service - privacy notice - NHS Digital

MEDICAL RESEARCH

With your consent, we will share information from medical records to support medical research when the law allows us to do so. For example, to learn more about why people get ill and what treatment might work best.

This is important because:

The use of information from GP medical records is very useful in developing new treatments and medicines.

Medical researchers use information from medical records to help answer important questions about illnesses and disease so that improvements can be made to the care and treatment patients receive

We share information with the following medical research organisations with your explicit consent or when the law allows: National Institute for Heath and Care Research

RESEARCH – OXFORD UNIVERSITY (Much Birch Surgery only)

This project focuses on utilising Large Language Models (LLMs) to generate accurate, evidence-based treatment recommendations and other clinical outputs, including referral letters and discharge summaries to develop an innovative AI model designed to reduce administrative workload for GPs which enhancing clinical decision-making.

From Much Birch Surgery we will provide an abstract of data to support the development of the LLM model. The pseudonymised abstract will offer insights into patient care workflows and structured/unstructured data management, aiding in refining the AI's capabilities.

Transfer of the data will be through a secure web-based SharePoint portal (as per NHS/GP instructions) and only a small number of approved researchers will be allowed to access and process the data. The research team do not hold the pseudonymisation key so the data it receives is considered anonymised in the hands of the recipient.

Oxford University relies on Article 6(1)(e) of the UK General Data Protection Regulation (UK GDPR) to process personal data where processing is necessary for a task carried out in the public interest or in the exercise of official authority vested in the University. In this instance the public interest task is research.

Oxford University also relies on Article 9(1)(j) of the UK GDPR to process special category data where processing is necessary for scientific research purposes.

This is in accordance with Article 89 of the UK GDPR which states that the research shall be subject to appropriate safeguards to ensure technical and organisational measures are in place – with a particular emphasis on data minimisation. This signed and agreed DPIA sets out those measures to ensure the lawful basis is engaged.

SAFEGUARDING

The PCN is dedicated to 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.

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…'*

Categories Of Personal Data

The data collected by staff in the event of a safeguarding situation will be as much personal information as is possible that is necessary to obtain to handle the situation. In addition to some basic demographic and contact details, we will also process details of what the safeguarding concern is. This is likely to be special category information (such as health information).

Sources of the Data

The PCN will either receive or collect information when someone contacts the organisation with safeguarding concerns, or we believe there may be safeguarding concerns and make enquiries to relevant providers.

Recipients of personal data

The information is used by the PCN when handling a safeguarding incident or concern. We may share information accordingly to ensure duty of care and investigation as required with other partners such as local authorities, the police or healthcare professionals (i.e. their GP or mental health team).

NATIONAL OPT-OUT FACILITY

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 confidential patient information helps to ensure you get the best possible care and treatment.

The confidential patient information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, 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 choose to opt out your confidential patient information will still be used to support your individual care.

We do not share your confidential patient information for purposes beyond your individual care without your permission. When sharing data for planning and reporting purposes, we use anonymised data so that you cannot be identified in which case your confidential patient information isn't required.

Information being used or shared for purposes beyond individual care does not include your confidential patient information being shared with insurance companies or used for marketing purposes and information would only be used in this way with your specific agreement.

Health and care organisations that process confidential patient information have to put systems and processes in place so they can be compliant with the national data opt-out. They must respect and apply your opt-out preference if they want to use or share your confidential patient information for purposes beyond your individual care.

The PCN is currently compliant with the national data-out policy as we do not share your confidential patient information for purposes beyond your individual care without your permission.

To find out more, please visit www.nhs.uk/your-nhs-datamatters

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 Manage Your Choice Registration Form.

  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.

You can change your choice at any time.

SUMMARY CARE RECORDS

Your Summary Care Record (SCR) is an electronic record of important patient information created from the GP medical records. It contains information about medications, allergies and any bad reactions to medications in the past. It can be seen by staff in other areas of the health and care system involved in your direct care.

During the height of the pandemic, changes were made to the SCR to make additional patient information available to all appropriate clinicians when and where they need it, to support direct patient care, leading to improves 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 have a SCR or opt back in to allow sharing of additional

information. Further details about the SCR and your choices can be found here - Summary Care Record supplementary transparency notice - NHS England Digital

NHS DIGITAL DATA COLLECTION FROM THE PCN

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

For example, patient data can help the NHS to:

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

In order to comply with its legal obligations, the PCN may send patient data, when directed by the Secretary of State for Health under the Health and Social Care Act 2012, for these purposes.

The PCN contributes to national clinical audits and will send the data, which is required by NHS England when the law allows. This may include demographic data such as date of birth and information about your health, which is recorded in coded form.

To find out more or to register your choice to opt out, please visit 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

SERVICE EVALUATION

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

The legal basis for contacting you to take part -

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

- *Article 9, (h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the*

employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems

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

- *Article 6(1)(a) - Consent of the data subject (you)*
- *Article 9(2)(a) – Explicit consent of the data subject. (you)*

ONLINE ACCESS & NHS APP

There will be certain protocols that we have to follow to give you online access, including written consent and the production of documents that prove your identity.

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

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

You will see all the information within your health record automatically. If you are over 16 and have an online account, such as through the NHS App, NHS website, or another online primary care service, you will be able to see all future notes and health records from your doctor (GP).

You will be able to see notes from your appointments, as well as test results and any letters that are saved on your records. This only applies to records from your doctor (GP), not from hospitals or other specialists. You will only be able to see information from 1st November 2023. For most people, access will be automatic, and you will not need to do anything

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

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

The NHS App, website and other online services are all very secure, so no one can access your information except you. You will need to make sure you protect your login details. Do not share your password with anyone as they will then have access to your personal information.

If you do not want to see your health record, or if you would like more information about these changes, please speak to your GP or reception staff at your registered practice.

iGPR - SUBJECT ACCESS REQUESTS & MEDICAL REPORTS

In some instances, we use a processor, iGPR Technologies Limited (iGPR) to assist us with responding to report requests relating to your patient data, such as subject access requests that you submit to us (or that someone acting on your behalf submits to us) and report requests that insurers submit to us under the Access to Medical Records Act 1988 in relation to a life insurance policy that you hold or that you are applying for.

iGPR manages the reporting process for us by reviewing and responding to requests in accordance with our instructions and all applicable laws, including UK data protection laws. The instructions we issue to iGPR include general instructions on responding to requests and specific instructions on issues that will require further consultation with the GP responsible for your care.

POPULATION HEALTH MANAGEMENT

Population Health Management (or PHM for short) is aimed at improving the health of an entire population. It is being implemented across the NHS and the PCN is taking part in Hereford and Worcestershire.

PHM is about improving the physical and mental health outcomes and wellbeing of people and making sure that access to services is fair, timely and equal. It helps to reduce the occurrence of ill-health and looks at all the wider factors that affect health and care.

The PHM approach requires health care organisations to work together with communities and partner agencies, for example, GP practices, community service providers, hospitals and other health and social care providers.

These organisations will share and combine information with each other in order to get a view of health and services for the population in a particular area. This information sharing is subject to robust security arrangements.

How will your personal data be used?

Information about your health care, which includes personal data, will be combined to create a picture of your health care.

Anything that can identify you will be removed and will be replaced with a unique code, so that people working on that data will only see the code and cannot see any personal data.

This means that the people working with the data will only see the code and cannot see which patient the information relates to.

If we see that an individual might benefit from some additional care or support, we will send the information back to your GP or hospital provider and they will use the code to identify you and offer you relevant services.

Examples of how the information could be used for several healthcare related activities include:

- improving the quality and standards of care provided
- research into the development of new treatments
- preventing illness and diseases
- monitoring safety
- planning services

Who will your personal data be shared with?

Your GP and other care providers will send the information they hold on their systems to the Midlands and Lancashire Commissioning Support Unit (MLCSU), who part of NHS England. More information can be found here NHS Midlands and Lancashire (midlandsandlancashirecsu.nhs.uk)

MLCSU will link all the information together. Your GP and other care providers will then review this information and make decisions about the whole population or particular patients that might need additional support.

MLCSU is legally obliged to protect your information and maintain confidentiality in the same way that your GP or hospital provider is.

Is using your personal data in this way lawful?

Health and Social Care Providers are permitted by data protection law to use personal information where it is 'necessary for medical purposes. This includes caring for you directly, as well as management of health services more generally.

Some of the work that happens at a national level with your pseudonymised personal information is enabled by other legislation. Sharing and using your information in this way helps 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, and, unless directly for your care, pseudonymised data is used so that you cannot be identified.

Can you object to your personal data being used as part of the Population Health Management project?

You have a right to object to your personal information being used in this way. If you do choose to 'opt out' please contact the practice. If you are happy for your personal information to be used as part of this project then you do not need to do anything further, although you do have the right to change your mind at any time.

If you still have concerns, you can also contact the Information Commissioner's Office directly at the following link https://ico.org.uk/make-a-complaint/your-personal-information-concerns/

OUR PRACTICE WEBSITES

Our practice websites use cookies to optimise your experience. Using this feature means that you 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 websites. The only websites this Privacy Notice applies to is the surgeries named within the PCN. 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.

TELEPHONE SYSTEM

Our telephone system records all telephone calls. Recordings are retained for up to three years and are used periodically for the purposes of seeking clarification where there is a dispute as to what was said and for staff training. Access to these recordings is restricted to named senior staff.

RECORDING AND TRANSCRIPTION

We may use recording and transcription tools during meetings to support accuracy and record-keeping. These processes do not collect or store personal identifiable data, and recordings are handled in line with our data protection obligations.

TEXT MESSAGES

If you have provided your mobile telephone number, we may use this to send automatic appointment reminders, appointment booking links, requests to complete surveys or to make you aware of services provided by the surgery that we feel will be to your benefit. If you do not wish to receive these text messages, please let the Reception Team know.

We use AccuRx desktop which is an accredited software solution that can be installed on practice computers and integrates with the patient record to allow text messages between the practice and patients.

Non-identifiable usage data is collected, retained and processed by AccuRx for service evaluation and improvement. The AccuRx solution has been assured by NHS Digital for IG and clinical safety.

Any medical or health related personal information will be treated with confidence in line with the common law duty of confidentiality and the Confidentiality NHS Code of Practice.

CCTV FOOTAGE

Your registered practice may use Close Circuit Television (CCTV) to record images within public areas of the practice for the safety and security of our patients and staff.

CCTV footage is managed in the same way as all other personal data processed by us and in line with current legislation.

MEDICAL EXAMINER SERVICE

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

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

Medical examiner offices are led by medical examiners, senior doctors from a range of specialties including general practice, who provide independent scrutiny of deaths not taken at the outset for coroner investigation. They put the bereaved at the centre of processes after the death of a patient, by giving families and next of kin an opportunity to ask questions and raise concerns. Medical examiners carry out a proportionate review of medical records and liaise with doctors completing the Medical Certificate of Cause of Death (MCCD). The PCN will share any patient information with the service upon request.

YOUR RIGHTS AS A PATIENT

Even if we already hold your personal data, you still have various rights in relation to it. Do please contact your registered practice if you would like to discuss this further. We will seek to deal with your request without undue delay, and in any event in accordance with the requirements of any applicable laws. Please note that we may keep a record of your communications to help us resolve any issues which you raise.

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. Detailed guidance is available within the practice's Subject Access Request Policy available on our websites or in hard copy on request. To apply for copies of your data, you need to do the following:

    - Your request should be made to your registered practice either by verbal request, in writing or via email

    - For information from a hospital or other Trust/NHS organisation you should write direct 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 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

Right to object: If we are using your data and you do not agree, you have the right to object. We will respond to your request within one month (although we may be allowed to extend this period in certain cases). This is NOT an absolute right sometimes we will need to process your data even if you object.

Right to withdraw consent: Where we have obtained your consent to process your personal data for certain activities (for example for a research project, or consent to send you information about us or matters you may be interested in), you may withdraw your consent at any time.

Right to erasure: In certain situations (for example, where we have processed your data unlawfully), you have the right to request us to "erase" your personal data. We will respond to your request within one month (although we may be allowed to extend this period in certain cases) and will only disagree with you if certain limited conditions apply. If we do agree to your request, we will delete your data but will need to keep a note of your name/ other basic details on our register of individuals who would prefer not to be contacted. This enables us to avoid contacting you in the future where your data are collected in unconnected circumstances. If you would prefer us not to do this, you are free to say so.

Right of data portability: If you wish, you have the right to transfer your data from us to another data controller. We will help with this with a GP-to-GP data transfer and transfer of your hard copy notes.

WHAT SHOULD YOU DO IF YOUR PERSONAL INFORMATION CHANGES?

You should tell us so that we can update our records please contact Reception at your registered practice as soon as any of your details change, this is especially important for changes of address or contact details (such as your mobile phone number). We will, from time to time, ask you to confirm that the information we currently hold is accurate and up to date.

OBJECTIONS/COMPLAINTS

Should you have any concerns about how your information is managed by the PCN, please contact your registered practice or our Data Protection Officer. If you are still unhappy following a review by your registered practice, you have a right to lodge a complaint with a supervisory authority:

Information Commissioner:
Wycliffe house, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel: 01625 545745
https://ico.org.uk/

If you are happy for your data to be used for the purposes described in this privacy notice, then you do not need to do anything. If you have any concerns about how your data is shared or would like to know more about your rights in respect of the personal data we hold about you, then please contact your registered practice.

DATA PROTECTION OFFICER

The PCN Data Protection Officer is Paul Couldrey of PCIG Consulting Limited.

Email: paul.couldrey@nhs.net
Postal: PCIG Consulting Limited
7 Westacre Drive, Quarry Bank, Dudley, West Midlands DY5 2EE

FURTHER INFORMATION

Further information about the way in which the NHS uses personal information and your rights in that respect can be found in:

- The NHS Care Record Guarantee
- The NHS Constitution
- NHS Digital's Guide to Confidentiality in Health & Social Care

IF ENGLISH IS NOT YOUR FIRST LANGUAGE

If English is not your first language, you can request a translation of this Privacy Notice.

CHANGES TO OUR PRIVACY NOTICE

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

This Privacy Notice was last updated on 12th June 2025.