DATA PROTECTION PRIVACY NOTICE FOR PATIENTS

INTRODUCTION

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

The UK General Data Protection Regulation (UKGDPR) and the Data Protection Act 2018 (DPA 2018) became law on 25th May 2018, and 1st January 2021 when the UK exited the EU.

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 Much Birch Surgery.

As a result, we have published this privacy notice to make it easier for you to find out how the NHS uses and protects your information.

WHAT IS A 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 (UKGDPR).

Under the UKGDPR, the organisation must process personal data in a fair and lawful manner and applies to everything that is done with patient's personal information. In practice, this means that the organisation must:

- have legitimate reasons for the use or collection of personal data
- not use the data in a way that may cause adverse effects on the individuals (e.g., improper sharing of their information with 3rd parties)
- be transparent about how you the data will be used, and give appropriate privacy notices when collecting their personal data
- handle personal data only as reasonably expected to do so
- make no unlawful use of the collected data

WHY ARE WE PROVIDING THIS PRIVACY NOTICE?

We are required to provide you with this Privacy Notice by Law. If you are unclear about how we process or use your personal and healthcare information, or you have any questions about this Privacy Notice or any other issue regarding your personal and healthcare information, then please do contact our Data Protection Officer.

Much Birch Surgery are bound by the UKGDPR 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 – the UKGDPR 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 must be clear and open with people about how their information is used.

Much Birch 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

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?

Much Birch Surgery will be what is known as the ‘Controller’ of your personal data under the Data Protection Act 2018. We 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.

NHS health records may be electronic, paper-based or a mixture of both. We use a combination of working practices and technology to ensure that your information is kept confidential and secure.

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 to the organisation
- Any contact the organisation and/or Much Birch Surgery 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.

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

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

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

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.

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. If a sub-contractor acts as a data processor for Much Birch Surgery an appropriate contract (Article 24-28) will be established for the processing of your information.

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), or where the law requires information to be passed on.

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 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.

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 Much Birch Surgery an appropriate contract (art 24-28) will be established for the processing of your information.

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

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 Much Birch Surgery 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. Much Birch Surgery also confirm 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

Much Birch Surgery has signed the National Data Sharing Arrangement (NDSA) for GP connect. GP Connect helps clinicians gain access to GP patient records during interactions away from a patient's registered practice and makes their medical

information available to appropriate health and social care professionals when and where they need it, to support the patient's direct care.

From a privacy, confidentiality and data protection perspective, GP Connect provides a method of secure information transfer and reduces the need to use less secure or less efficient methods of transferring information, such as email or telephone.

GP Connect - Key Points

- GP Connect can only be used for direct care purposes.
- Individuals can opt out of their GP patient record being shared via GP Connect by contacting their GP practice.
- Access to GP Connect is governed by role-based access control (RBAC) and organisational controls; only people who need to see the GP patient record for a patient's direct care should be able to see it.
- All systems that allow the use of GP Connect must undergo a robust compliance process and the organisations involved must sign a connection agreement holding them to high standards of information security.

GP Connect products can help health and social care professionals share, view or act on information that could be required for a patient's direct care, but they would otherwise have difficulty accessing easily (for example if they are using different IT systems).

Organisations can have access to relevant information in GP patient records to provide direct care to patients only.

Type of organisations that use GP Connect

Examples of organisations that may wish to use GP connect to view GP patient records include:

- GP surgeries that patients are not registered at - for example, if they need to see a doctor when they are away from home
- Secondary care (hospitals) if they need to attend A&E or are having an operation
- GP hubs/primary care networks (PCNs)/integrated care systems (ICS), partnerships between healthcare providers and local authorities
- Local 'shared care' record systems
- Ambulance trusts, so paramedics can view GP patient records in an emergency
- Healthcare professionals such as community services
- Acute and emergency care service providers
- NHS 111
- Pharmacies
- Optometrists
- Dentistry
- Mental health trusts
- Hospices
- Adult and children's social care
- Care and nursing homes

All access to your GP patient record is stored within an audit trail at your GP practice and within the organisation that information has been shared with.

Confidentiality

Confidentiality and trust are essential to the relationship between GPs and their patients. The information a patient provides to their GP is confidential, and they can expect that any information that is shared for their direct care will remain confidential. GP Connect relies on 'implied consent'

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.

The NDSA and its terms and conditions stipulate that any information received or accessed about a patient for direct care purposes must remain confidential.

In addition to the NDSA, health and social care professionals are also subject to their own professional codes of confidentiality and are aware that any information received via GP Connect is provided in confidence, which must be respected.

Organisations using GP Connect are notified of their duty as 'controllers' to be fair and transparent about their processing of their patients' information and to ensure that their transparency notices are fully updated with how they may be using GP Connect functionality.

NHS England helps support the mitigation of information sharing risks by ensuring that:

- NHS England audit data access is subject to two-factor authentication and role-based access controls - only certain assured users can have access to the full audit logs

- a completed Supplier Conformance Assessment List (SCAL) which covers service and capability specific compliance requirements and controls of the consumer system is in place

It is the responsibility of organisations using GP Connect to ensure that they comply with the NDSA, and their statutory and legal obligations regarding data protection and confidentiality.

Opting out of GP Connect

If patients do not wish their information to be shared using GP Connect, they can opt out by contacting their GP practice.

National Data Opt-Out

The National Data Opt-out is a service that allows patients to opt out of their confidential patient information being used for research and planning (see section below).

The National Data Opt-out only applies to any disclosure of data for purposes beyond direct care, so having National Data Opt-out will not prevent your GP patient record being shared via GP Connect.

ACCESSING APPOINTMENTS

When and how can you contact your general practice?

Your general practice is open from **8.00am to 6.30pm, Monday to Friday**. Throughout these hours you, or your carer on your behalf, can:

- Visit the practice
- Call them
- Go online using the practice's website or the NHS App.

You can choose the way you contact your practice based on what is best for you. Some practices may have longer hours or may ask that you contact them via phone or in person for urgent queries.

What if the practice is closed?

If you need urgent help for your physical or mental health when the general practice is closed, and you cannot wait until they open, go online to 111.nhs.uk or call 111. They will tell you what to do next.

What if it's an emergency?

If it's a serious or life-threatening emergency, go straight to A&E (Accident and Emergency) or call 999.

What happens when you contact your practice to request an appointment?

Whether you make your request by phone, on-line or visiting your practice, you may be asked to give your practice some details so that they can assess what is best for you based on your clinical need. The practice team will consider your request for an appointment or medical advice and tell you within one working day what will happen next.

This could be:

- An appointment that day or a subsequent day
- A phone call that day or a subsequent day
- A text message responding to your query
- Advice to go to a pharmacy or another NHS service

Your practice will decide what is best for you based on your clinical need. Your practice cannot tell you to just call back the next day.

Who might help you?

You might be offered a face-to-face appointment or a phone call with a GP or other member of the practice staff, like a nurse or pharmacist.

If you have a carer, they can speak for you with your consent.

You can ask to see a preferred healthcare professional, and the practice will try to meet your request, although you might have to wait longer for that person to be available.

It can be helpful to see the same healthcare professional, particularly if you have a long-term health condition.

From what age can you see a GP on your own?

If you are 16 or older, you can make and go to appointments by yourself. If you are under 16, you can still ask to see a GP without your parent or guardian. The GP will decide if that's appropriate for you.

What if you need extra help?

If you do not speak English, you can ask for interpretation services in your preferred language when you make an appointment.

If you need extra help like longer appointments, a quiet space, wheelchair access, or information in a different format, tell your practice and they will try to help.

How do you choose a general practice?

You can:

- Call or visit a local practice
- Use Find a GP online

If you want to change to a new general practice, you can do so at any point. Most people have a few choices nearby.

Do you need ID or proof of address?

No, you do not need ID, an NHS number or proof of address. It can help the practice if you do, but it is not needed to register or see a GP. You can also register with a practice if you are homeless.

Can a practice say no to registering you?

They must write to you within 14 days if they say no and explain why. A practice can only say no for a good reason, like if you live too far away or their patient list is closed. For example, they cannot say no for reasons such as immigration status, not having a permanent address, or for reasons connected with other characteristics protected under equalities legislation.

Can you choose which hospital or clinic you are referred to?

If your GP needs to refer you for a physical or mental health condition, in most cases you have the right to choose the hospital or service you'd like to go to. You can get further information on your right to choose on the nhs.uk website.

If you are new to the UK

You can still register with a GP. It's free to use and your immigration status does not affect your right to register with a GP.

If you are away from home but still in the UK

If you are away from home for more than 24 hours (but less than 3 months), you can register as a temporary patient near where you're staying.

You can also change your nominated pharmacy so you can get your medicine nearby. You can do this by contacting your practice or via the NHS App.

Do general practices charge for anything?

NHS GP services are free. Sometimes, if you ask the GP to do private work (like writing a letter for insurance), they may charge a fee.

How should everyone be treated?

The practice should treat everyone fairly, kindly and respectfully. Likewise, you should also treat staff with respect. The practice can remove patients from their list if they are violent or abusive to staff.

To learn more about your rights, you can read the NHS Constitution.

How can you help your general practice?

- Be prepared: Before an appointment, think about writing down your symptoms, what you are worried about and what you want to talk about.

- Be on time: Being late for an appointment or being unavailable for a timed call-back can affect other patients.

- Cancel if needed: If you can't go to your appointment, tell the practice as soon as you can, so that they can offer it to someone else.

- Use the NHS App or website: If you're confident using smart phones or computers, you can book or cancel appointments, order repeat prescriptions, and see your test results online.

- Turn on notifications: If you use the NHS App, turn on notifications so the practice can contact you more easily. Please keep an eye out for messages.

- Order repeat medicines on time: Make sure you ask for repeat prescriptions on time, so you don't run out, and only order what you need.

- Join the Patient Participation Group: You practice will have a group of patients who can offer feedback on the services it delivers. Your practice website should explain how you can join.

How can you give feedback or raise concerns?

If you want to give feedback, raise a concern or wish to make a formal complaint, ask to speak to the practice manager. If you don't feel comfortable doing this, contact your integrated care board (ICB) – the local NHS body that oversees GPs practices. You can find your local integrated care on the NHS England website.

You can also give feedback about your practice to your local Healthwatch. Their job is to make sure NHS leaders and other decision-makers hear your voice and use your feedback to improve care. Healthwatch is independent and impartial, and any information you share with them is confidential. To find your local Healthwatch visit the Healthwatch website.

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 Much Birch Surgery 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.

AUDIT

Auditing of clinical notes is done by Much Birch Surgery as part of their commitment to effective management of healthcare whilst acting as data controller/processor for your GP practice.

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

Much Birch Surgery 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 the Practice.

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

The following provisions of the 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.

ANONYMISED INFORMATION

Sometimes we may provide information about you in an anonymised form. Such information is used 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.

RESEARCH - NATIONAL INSTITUTE FOR HEALTH & SOCIAL CARE RESEARCH (NIHR) - CLINICAL RESEARCH NETWORK

Clinical Research Network West Midlands (CRN WM) provides a research delivery service to GP practices across the West Midlands. All CRN WM Delivery Support staff are employed by The Royal Wolverhampton NHS Trust. All NHS Staff members who have been allocated to work within Much Birch Surgery will be issued with a Letter of access or assurance to confirm individual study placements and pre-employment checks.

The legal bases for processing this information

CRN WM processes data under the instruction of the individual research protocol, as delegated by the practice (data controller). You can opt out of being invited to participate in research at any time, please inform a member of the practice team and we will add the appropriate opt out code to your record.

Prior to informed consent:

The legal basis which allows us to process your personal data for research is GDPR article 6 (1)(f) …legitimate interests…except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject…'

Once informed consent has been given:

The legal basis which allows us to process your personal data is informed consent - Article 6 1(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; and Article 9 (2) (a) the data subject has given explicit consent to the processing those personal data for one or more specified purposes.

Individual study consent forms will detail how to withdraw consent and who to contact, this will usually be via the study sponsor.

Categories of personal data

The data processed by CRN WM delivery staff, in addition to demographic and contact details, is likely to be special category information (such as health information) to determine eligibility for individual research studies.

Recipients of data

The data processed by CRN WM delivery staff will be used to invite potentially eligible patients into research studies. Once patients have consented to participate, data processed by the CRN WM delivery staff will be used to answer the research questions as outlined in individual research protocols.

For further information, please refer to the Clinical Research Network West Midlands Privacy Notice.

RESEARCH – OXFORD UNIVERSITY

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.

PATIENT COMMUNICATION

Because we are obliged to protect any confidential information, we hold about you and we take this very seriously, 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 if we need to notify you about appointments and other services that we provide to you involving your direct care, therefore you must ensure that we have your up-to-date details. 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 give us permission to contact you via SMS if you have provided us with your mobile telephone number. Please let us 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. Please ensure that we have your up-to-date details.

There may be occasions where authorised research facilities would like you to take part in research. Your contact details may be used to invite you to receive further information about such research opportunities.

SAFEGUARDING

Much Birch Surgery 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 the General Data Protection Regulation (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 Much Birch Surgery 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

Much Birch Surgery 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 Much Birch Surgery 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).

THIRD PARTY PROCESSORS

To deliver the best possible service, Much Birch Surgery will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition, Much Birch Surgery 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 website 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 to the Data Protection Officer as below.

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 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.

SUMMARY CARE RECORDS

All patients registered with a GP have a Summary Care Record, unless they have chosen not to have one. The information held in your Summary Care Record gives registered and regulated healthcare professionals, away from your usual GP practice, access to information to provide you with safer care, reduce the risk of prescribing errors and improve your patient experience.

Your Summary Care Record contains basic (Core) information about allergies and medications and any reactions that you have had to medication in the past.

Some patients, including many with long term health conditions, previously have agreed to have Additional Information shared as part of their Summary Care Record. This Additional Information includes information about significant medical history (past and present), reasons for medications, care plan information and immunisations.

Change to information held in your Summary Care Record

The Department of Health and Social Care has removed the requirement for a patient's prior explicit consent to share Additional Information as part of the Summary Care Record.

This is because the Secretary of State for Health and Social Care has issued a legal notice to healthcare bodies requiring them to share confidential patient information with other healthcare bodies where this is required to diagnose, control and prevent the spread of the virus and manage the pandemic. This includes sharing Additional Information through Summary Care Records, unless a patient objects to this.

If you have already expressed a preference to only have Core information shared in your Summary Care Record, or to opt-out completely of having a Summary Care Record, these preferences will continue to be respected and this change will not apply to you. For everyone else, the Summary Care Record will be updated to include the

Why the Department of Health & Social Care have made this change

To look after your health and care needs, health and social care bodies may share your confidential patient information contained in your Summary Care Record with clinical and non-clinical staff in other health and care organisations, for example hospitals, NHS 111 and out of hours organisations. These changes will improve the healthcare that you receive away from your usual GP practice.

Your rights in relation to your Summary Care Record

Regardless of your past decisions about your Summary Care Record preferences, you will still have the same options that you currently have in place to opt out of having a Summary Care Record, including the opportunity to opt-back in to having a Summary Care Record or opt back in to allow sharing of Additional Information.

You can exercise these rights by doing the following:

- **Choose to have a Summary Care Record with all information shared**. This means that any authorised, registered and regulated health and care professionals will be able to see a detailed Summary Care Record, including Core and Additional Information, if they need to provide you with direct care.

- **Choose to have a Summary Care Record 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 Summary Care Record if they need to provide you with direct care.

- **Choose to opt-out of having a Summary Care Record 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 the reception team at Much Birch Surgery or complete this form and return it to the practice.

NHS DIGITAL DATA COLLECTION FROM THE PRACTICE

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

For example, patient data can help the NHS to:

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

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

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

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

NHS Digital Purposes for Processing Patient Data

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

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

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

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

What Patient Data NHS Digital Collect

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

While 1 September has been seen by some as a cut-off date for opt-out, after which data extraction would begin, Government has stated this will not be the case and data extraction will not commence until NHS Digital have met the tests.

The NHS is introducing three changes to the opt-out system which mean that patients will be able to change their opt-out status at any time:

- Patients do not need to register a Type 1 opt-out by 1 September to ensure their GP data will not be uploaded

- NHS Digital will create the technical means to allow GP data that has previously been uploaded to the system via the GPDPR collection to be deleted when someone registers a Type 1 opt-out

- The plan to retire Type 1 opt-outs will be deferred for at least 12 months while we get the new arrangements up and running, and will not be implemented without consultation with the RCGP, the BMA and the National Data Guardian

NHSD 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, full postcode and date of birth, is replaced with unique codes which 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 in the data. The diagram below helps to explain what this means. Using the terms in the diagram, the data we collect would be described as de-personalised.

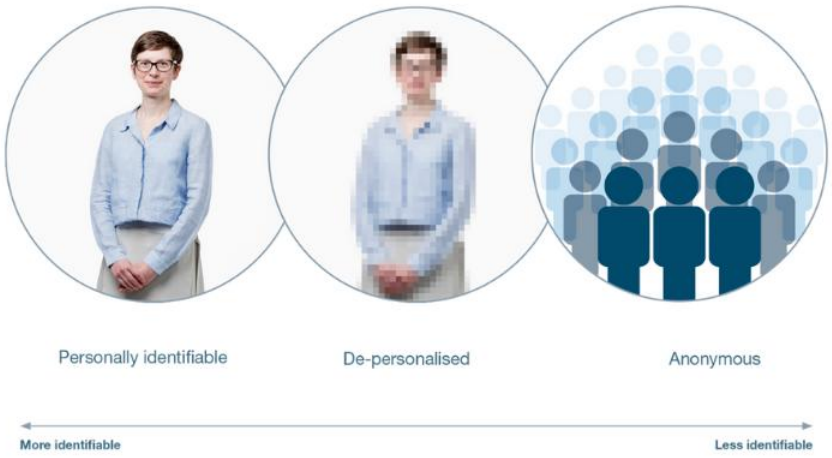

Image provided by Understanding Patient Data under licence.

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

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

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

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

The Data NHS Digital collects

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

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

NHS Digital will 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 staff who have treated you

More detailed information about the patient data we collect is contained in the Data Provision Notice issued to GP practices.

NHS Digital Does 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

Opting Out of NHS Digital Collecting Your Data (Type 1 Opt-Out)

If you do not want your identifiable patient data (personally identifiable data in the diagram above) to be shared outside of your GP practice for purposes except for your own care, you can register an opt-out with your GP practice. This is known as a Type 1 Opt-out.

Type 1 Opt-outs were introduced in 2013 for data sharing from GP practices but may be discontinued in the future as a new opt-out has since been introduced to cover the broader health and care system, called the National Data Opt-out. If this happens people who have registered a Type 1 Opt-out will be informed. More about National Data Opt-outs is in the section Who we share patient data with.

NHS Digital will not collect any patient data for patients who have already registered a Type 1 Opt-out in line with current policy. If this changes patients who have registered a Type 1 Opt-out will be informed.

If you do not want your patient data shared with NHS Digital, you can register a Type 1 Opt-out with your GP practice. You can register a Type 1 Opt-out at any time. You can also change your mind at any time and withdraw a Type 1 Opt-out.
Data sharing with NHS Digital started on 1 September 2021.

If you have already registered a Type 1 Opt-out with Much Birch Surgery your data will not be shared with NHS Digital.

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

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

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

NHS Digital Legal Basis for Collecting, Analysing, and Sharing Patient Data

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

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

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

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

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

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

How NHS Digital use 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 you 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 we 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. We never publish any patient data that could identify you. All data we publish is anonymous statistical data.

For more information about data, we publish see Data and Information and Data Dashboards.

We may also carry out analysis on national data sets for data quality purposes and to support the work of others for the purposes set out in Our purposes for processing patient data section above.

Who Does NHS Digital Share Patient Data With?

All data which 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 who 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), Integrated Care Boards (ICBs) and integrated care organisations (ICOs)
- local authorities
- research organisations, including universities, charities, clinical research organisations that run clinical trials and pharmaceutical companies

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

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

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

This would include:

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

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

out policy before any identifiable patient data (personally identifiable data in the diagram above) about you was shared.

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

Much Birch Surgery is one of many organisations working in the health and care system to improve care for patients and the public).

Whenever you use a health or care service, such as attending Accident & Emergency or using Community Care services, important information about you is collected in a patient record for that service. Collecting this information helps to ensure you get the best possible care and treatment.

The information collected about you when you use these services can also be used and provided to other organisations for purposes beyond your individual care, for instance to help with:

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

This may only take place when there is a clear legal basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential patient information about your health and care is **only used** like this as allowed by law.

Most of the time, anonymised data is used for research and planning so that you cannot be identified in which case your confidential patient information is not needed.

You have a choice about whether you want your confidential patient information to be used in this way. If you are happy with this use of information you do not need to do anything. If you do choose to opt out your confidential patient information will still be used to support your individual care.

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

You can also find out more about how patient information is used at:

NHS Health Research Authority (which covers health and care research)

and

Understanding Patient Data - What You Need to Know (which covers how and why patient information is used, the safeguards and how decisions are made)

You can change your mind about your choice at any time. Data being used or shared for purposes beyond individual care does not include your data being shared with insurance companies or used for marketing purposes and data would only be used in this way with your specific agreement.

Where NHS Digital stores 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 you to be directly or indirectly identified), for example statistical data that is published, may be stored and processed outside of the UK. Some of our processors may process patient data outside of the UK. If they do, we will always ensure that the transfer outside of the UK complies with data protection laws.

EMIS WEB

Much Birch Surgery uses a clinical system provided by a data processor called EMIS. EMIS started storing Much Birch Surgery's EMIS Web data in a highly secure, third-party cloud hosted environment, namely Amazon Web Services ("AWS").

The 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.

SHARED CARE RECORDS

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

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

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.

Much Birch Surgery is a member of South & West Herefordshire PCN. Other members of the network are:

- 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 Much Birch Surgery may share your information with other practices within the PCN to provide you with your care and treatment.

EXTENDED ACCESS

Taurus Healthcare provides extended access services to our patients which means you can access medical services outside of our normal working hours. In order to provide you with this service, we have formal arrangements in place with the Integrated Care Board (ICB) whereby certain key 'hub' practices offer this service for you as a patient to access outside of our opening hours. This means those key 'hub' practices will have to have access to your medical record to be able to offer you the service. Please note to ensure that those practices 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.

The key 'hub' practices are currently Station Medical Centre, Hereford; Ryeland Surgery, Leominster; Ross Community Hospital, Ross on Wye; The Medical Practice, Kington; Ledbury Health Partnership, Ledbury; Nunwell Surgery, Bromyard; Much Birch Surgery, Much Birch; Kingstone Surgery, Kingstone; Cradley Surgery, Cradley and Weobley Surgery, Weobley.

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)*

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.

ONLINE ACCESS & NHS APP

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

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

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 can now see all the information within your health record automatically. If you are over 16 and have an online account, such as through the NHS App, NHS website, or another online primary care service, you will now be able to see all future notes and health records from your doctor (GP). Some people can already access this feature, this will not change for you.

This means that you will be able to see notes from your appointments, as well as test results and any letters that are saved on your records. This only applies to records from your doctor (GP), not from hospitals or other specialists. You will only be able to see information from 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.

We use the NHS Account Messaging Service provided by NHS England to send you messages relating to your health and care. You need to be an NHS App user to receive these messages. Further information about the service can be found managed by NHS England.

SUBJECT ACCESS REQUESTS & MEDICAL REPORTS

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 this Practice 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 a number of 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 WEBSITE

Our website does 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 website. The only website this Privacy Notice applies to is the Much Birch 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.

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.

MEDICAL EXAMINER SERVICE

Following the death of any patients of Much Birch Surgery 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). Much Birch Surgery will share any patient information with the service upon request.

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.

YOUR RIGHTS AS A PATIENT

Even if we already hold your personal data, you still have various rights in relation to it. To get in touch about these, please contact us. 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 our Subject Access Request Policy available on our website 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 Much Birch Surgery either by verbal request, in writing or via email to Admin.muchbirch@nhs.net

    - 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 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), Much Birch Surgery 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 at Much Birch Surgery, please contact the Operations Manager or the Data Protection Officer as above. If you are still unhappy following a review by Much Birch Surgery, you have a right to lodge a complaint with a supervisory authority: You have a right to complain to the UK supervisory Authority as below.

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, then please contact the Data Protection Officer.

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

DATA PROTECTION OFFICER

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

Email: Couldrey@me.com
Postal: PCIG Consulting Limited
7 Westacre Drive, Quarry Bank, Dudley, West Midlands DY5 2EE

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 2nd October 2025.