LEDBURY HEALTH PARTNERSHIP

PRIVACY NOTICE FOR PATIENTS

HOW WE USE YOUR INFORMATION

Ledbury Health Partnership 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.

Please read this Privacy Notice carefully, as it contains important information about how we use the personal and healthcare information we collect on your behalf.

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018) became law on 25th May 2018. The UK GDPR is a UK regulation on the protection of confidential and sensitive (special) information, the DPA 2018 came into force in the UK on the 25th May 2018, repealing the previous Data Protection Act (1998).

For the purpose of applicable data protection legislation (including but not limited to the UK General Data Protection Regulation (Regulation (EU) 2016/679) (the "UK GDPR"), and the Data Protection Act 2018 we, are responsible for your personal data.

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

WHY ARE WE PROVIDING THIS PRIVACY NOTICE?
We are required to provide you with this Privacy Notice by Law. It explains how we use the personal and healthcare information we collect, store and hold about you. 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.

The Law says:

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

WHAT IS A PRIVACY NOTICE?
A Privacy Notice (or 'Fair Processing Notice') 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 new UK General Data Protection Regulations (UK GDPR).

Under the UK GDPR, 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

LEGAL JUSTIFICATION FOR COLLECTING AND USING YOUR INFORMATION
The Law says we need a legal basis to handle your personal and healthcare information.

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

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

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

WHO IS THE DATA CONTROLLER?

Ledbury Health Partnership is registered as a Data Controller under the Data Protection Act 2018. The registration number is **ZB105751** and can be viewed online in the public register at https://ico.org.uk. 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. The purposes for which we use your information are set out in this Privacy Notice.

FAIR PROCESSING

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

This Privacy Notice explains why we as an organisation collect information about our patients and how that information may be used.

Ledbury Health Partnership 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:

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

The Health and Social Care Act 2012 changed the way that personal confidential data is processed, 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.

HOW WE USE THE INFORMATION ABOUT YOU

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 the course of your diagnosis or treatment or ongoing 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.

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 clear consent to do so.

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 clear consent to do so.

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

HOW LONG WE KEEP YOUR PERSONAL INFORMATION

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

More information on records retention can be found online at:

NHS Records Management - Code of Practice 2020

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.

Ledbury Health Partnership uses a clinical system provided by a Data Processor called EMIS. With effect from 10th June 2019, EMIS started storing the organisation's EMIS Web data in a highly secure, third party cloud hosted environment, namely Amazon Web Services ("AWS").

The data will remain in the UK at all times 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.

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 your practice has had with you, including appointments (emergency or scheduled), clinic visits, etc.
- Notes and reports about your health, details of diagnosis and consultations with our GPs and other Health Professionals within the healthcare environment involved in your direct healthcare
- Details about treatment and care received
- Results of investigations, such as laboratory tests, x-rays, etc.
- Relevant information from other health professionals, relatives or those who care for you
- Recordings of telephone conversations between yourself and the organisation

INFORMATION ABOUT YOU FROM OTHERS

The organisation collects and holds data for the sole purpose of providing healthcare services to our patients and we will ensure that the information is kept confidential. However, we can disclose personal information if:

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

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

Information may be used for clinical audit purposes to monitor the quality of service provided, and may be held centrally and used for statistical purposes. Where we do this, we ensure that patient records cannot be identified.

Sometimes your information may be requested to be used for clinical research purposes – the organisation will always endeavour to gain your consent before releasing the information.

Improvements in information technology are also making it possible for us to share data with other healthcare providers with the objective of providing you with better care.

Patients can choose to withdraw their consent to their data being used in this way. When the organisation is about to participate in any new data-sharing scheme we will make patients aware by displaying prominent notices and on our website at least four weeks before the scheme is due to start. We will also explain clearly what you have to do to 'opt-out' of each new scheme.

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

HOW DO WE MAINTAIN THE CONFIDENTIALITY OF YOUR RECORDS?

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

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

We maintain our duty of confidentiality to you at all times. We will only ever use or pass on information about you if others involved in your care have a genuine need for it. We will not disclose your information to any third party without your permission unless there are exceptional circumstances (i.e. life or death situations), or where the law requires information to be passed on.

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.

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.

WHO WE MAY PROVIDE YOUR PERSONAL INFORMATION TO AND WHY?

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 where 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 in order to ensure they may properly deliver their services to you:

- Hospital professionals (such as doctors, consultants, nurses etc)
- Other GPs/Doctors
- Primary Care Networks
- Taurus Healthcare (Extended Hours Service)
- NHS Trusts/Foundation Trusts/Specialist Trusts
- NHS Commissioning Support Units
- NHS England (NHSE) and NHS Digital (NHSD)
- Multi-Agency Safeguarding Hub (MASH)
- Independent Contractors such as dentists, opticians, pharmacists
- Any other person 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
- Ambulance Trusts
- Integrated Care Systems
- Clinical Commissioning Groups
- Local Authorities
- Fire and Rescue Services
- Police & Judicial Services
- Social Care Services
- Education Services
- 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.

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

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

- Extended Access – we provide 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 Clinical Commissioning Group 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 South Wye Medical Centre, Hereford; The Marches Surgery, Leominster; Pendeen Surgery, Ross on Wye; The Medical Practice, Kington; Ledbury Health Partnership, Ledbury and Nunwell Surgery, Bromyard.

- Data Extraction by the Clinical Commissioning Group – the Clinical Commissioning Group at times extracts medical information about you, but the information we pass to them via our computer systems cannot identify you to them. This information only refers to you by way of a code that only your own practice can identify (it is pseudo-anonymised). This therefore protects you from anyone who may have access to this information at the Clinical Commissioning Group from ever identifying you as a result of seeing the medical information and we will never give them the information that would enable them to do this.

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

  Health information is shared with:

  - Wye Valley NHS Trust (including community services)

- St. Michael's Hospice
- Herefordshire Mental Health and Learning Disability Services
- Your registered general practice within Herefordshire

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

www.herefordshireccg.nhs.uk/your-services/herefordshire-one-record

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

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

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

You do not need to do anything if you are happy about how your confidential patient information is used.
If you do not want your confidential patient information to be used for research and planning, you can choose to opt out by using one of the following:

- Online service – Patients registering need to know their NHS number or their postcode as registered at their GP Practice

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

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

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

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

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

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

This collection will start from 1 September 2021. 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

We 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.

The Data NHD Digital collect

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

Data that directly identifies you as an individual patient, including your NHS number, General Practice Local Patient Number, full postcode, date of birth and if relevant date of

death, is replaced with unique codes produced by de-identification software before it is sent to NHS Digital. This means that no one will be able to directly identify you in the data. NHS Digital will be able to use the software to convert the unique codes back to data that could directly identify you in certain circumstances, and where there is a valid legal reason. This would mean that the data became personally identifiable in the diagram above. It will still be held securely and protected, including when it is shared by NHS Digital.

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 will start on 1 September 2021.

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

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

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

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

NHS Digital Legal Basis For Collecting, Analysing And Sharing Patient Data

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

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

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

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

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

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

How NHS Digital 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 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 a number of 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), clinical commissioning groups (CCGs) and integrated care organisations (ICOs)
- local authorities
- research organisations, including universities, charities, clinical research organisations that run clinical trials and pharmaceutical companies

If the request is approved, the data will either be made available within a secure data access environment within 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.

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.

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.

THIRD PARTY PROCESSORS

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

- 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)

- Further details regarding specific third-party processors can be supplied on request to the Data Protection Officer as below.

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

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 Ledbury Health Partnership an appropriate contract (art 24-28) will be established for the processing of your information.

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

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

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. To request this, you need to do the following:

    - Your request should be made to the Practice Manager at Ledbury Health Partnership
    - 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 have to make an administrative charge for any extra copies if the information requested is excessive, complex or repetitive
    - We are required to provide you with information within one month. We would ask therefore that any requests you make are in writing and it is made clear to us what and how much information you require
    - You will need to give adequate information (for example full name, address, date of birth, NHS number and details of your request) so that your identity can be verified, and your records located

- ***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 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 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. You have the right to request that your personal and/or healthcare information is transferred, in an electronic form (or other form) to another organisation, but we will require your clear consent to be able to do this.

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.

IF ENGLISH IS NOT YOUR FIRST LANGUAGE
If English is not your first language you can request a translation of this Privacy Notice.

TEXT MESSAGING AND CONTACTING YOU
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 in the event that 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 up to date details. This is to ensure we are actually contacting you and not another person.

ORGANISATION 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 Ledbury Health Partnership 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.

GP CONNECT SERVICE
The GP Connect service allows authorised clinical staff at NHS 111 to seamlessly access our clinical system and book directly on behalf of a patient. This means that should you call NHS 111 and the clinician believes you need an appointment the clinician will access available appointment slots only (through GP Connect) and book you in. This will save you time as you will not need to contact the organisation direct for an appointment.

Ledbury Health Partnership will not be sharing any of your data and the organisation will only allow NHS 111 to see available appointment slots. They will not even have access to

your record. However, NHS 111 will share any relevant data with us, but you will be made aware of this. This will help in knowing what treatment/service/help you may require.

Please note if you no longer require the appointment or need to change the date and time for any reason you will need to speak to one of our reception staff and not NHS 111.

MEDICINES MANAGEMENT
Ledbury Health Partnership 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 CCGs Medicines Management Team under a Data Processing contract with the Practice.

ONLINE ACCESS
You may ask us if you wish to have online access to your medical record. However, there will be certain protocols that we have to follow in order to give you online access, including written consent and 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.

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 your own GP practice know immediately if you change any of your contact details.

We may contact you using SMS texting to your mobile phone in the event that we need to notify you about appointments and other services that we provide to you involving your direct care. This is to ensure we are sure we are actually 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 your mobile telephone number. Please let your GP practice 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.

RESEARCH
Clinical Practice Research Datalink (CPRD) collects de-identified patient data from a network of GP practices across the UK. Primary care data are linked to a range of other health related data to provide a longitudinal, representative UK population health dataset. You can opt out of your information being used for research purposes at any time (see below), full details can be found here:

https://cprd.com/transparency-information

CPRD do not hold or process personal data on patients; however, NHS Digital (formally the Health and Social Care Centre) may process 'personal data' for us as an accredited

'safe haven' or 'trusted third-party' within the NHS when linking GP data with data from other sources. The legal bases for processing this data are:

- Medicines and medical device monitoring: Article 6(e) and Article 9(2)(i) - public interest in the area of public health
- Medical research and statistics: Article 6(e) and Article 9(2)(j) - public interest and scientific research purposes

Any data CPRD hold or pass on to bona fide researchers, except for clinical research studies, will have been anonymised in accordance with the Information Commissioner's Office Anonymisation Code of Practice. We will hold data indefinitely for the benefit of future research, but studies will normally only hold the data we release to them for twelve months.

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 GP Practice. 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 the practice for further information about opt out.

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

AUDIT

Auditing of clinical notes is done by Ledbury Health Partnership as part of their commitment to effective management of healthcare.

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

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

Auditing clinical management is no different to a multi-disciplinary team meeting discussion whereby management is reviewed and agreed. It would be realistically impossible to require consent for every patient reviewed which is unnecessary.

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

SAFEGUARDING

The organisation 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…'

The data collected by Practice staff in the event of a safeguarding situation will be as much personal information as is possible that is necessary to obtain in order 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).

The Practice 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.

The information is used by the Practice 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).

Safeguarding information such as referrals to safeguarding teams is retained by Ledbury Health Partnership when handling a safeguarding concern or incident. 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).

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. All areas within England are covered by a PCN.

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

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

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

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

CCTV RECORDING
CCTV is installed on our practice premises covering both the external area of the building and the internal area excluding consulting rooms. Images are held to improve the personal security of patients and staff whilst on the premises, and for the prevention and detection of crime. The images are recorded onto an integral hard drive of the equipment and are overwritten on a rolling basis. Viewing of these digital images is password protected and controlled by the Practice Manager.

OBJECTIONS AND/OR COMPLAINTS
Should you have any concerns about how your information is managed at Ledbury Health Partnership, please contact the Practice Manager. If you are still unhappy following a review by the organisation, you can then complain to the Information Commissioner's Office (ICO) via their website (www.ico.gov.uk) Telephone: 0303 123 1113

The Information Commissioner's Office is the Regulator for the General Data Processing Regulations and offer independent advice and guidance on the law and personal data, including your rights and how to access your personal information.

DATA PROTECTION OFFICER
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 Practice Data Protection Officer.

The organisation's 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

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

- The NHS Care Record Guarantee : http://www.nigb.nhs.uk/pubs/nhscrg.pdf
- The NHS Constitution : hhttp://www.wales.nhs.uk/nhswalesaboutus/thecoreprinciplesofnhswales
- NHS Digital's Guide to Confidentiality in Health & Social Care gives more information on the rules around information sharing : http://content.digital.nhs.uk/article/4979/Assuring-information

WHERE TO FIND OUR PRIVACY NOTICE

You may find a copy of this Privacy Notice on our website or a copy may be provided on request.

CHANGES TO OUR PRIVACY NOTICE

It is important to note 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 28th June 2021.