PCIG Consulting Template

Practice Privacy Notice

SystemOne Practices

Version: **2.5**
Date: **27/06/2022**

This template is for use by Practices to Comply with the UKGDPR requirement to display a Privacy Notice regarding processing of patient data. The template is Generic in design as PCIG Consulting have clients across the UK, local sharing arrangements and area specific sharing or processing will need to be added by the practice.

This may include Area Specific Sharing such as:

Nottingham CCG
MIG
Healthcare Portal
GPRCC
Population Health Management Programme

Derbyshire CCG
Population Health Management Programme

Dudley CCG
POD
PCN

Lime Grove Medical Centre Matlock (the Practice)

Data Protection Privacy Notice for Patients

Introduction:

This privacy notice lets you know what happens to any personal data that you give to us, or any information that we may collect from you or about you from other organisations.

This privacy notice applies to personal information processed by or on behalf of the practice.

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 practice responsible for your personal data is Lime Grove Medical Centre Matlock.

This Notice describes how we collect, use and process your personal data, and how in doing so, we comply with our legal obligations to you. Your privacy is important to us, and we are committed to protecting and safeguarding your data privacy rights.

How we use your information and the law.

Lime Grove Medical Centre Matlock will be what's known as the 'Controller' of your personal data.

We collect basic personal data about you and location-based information. This does include name, address and contact details such as email and mobile number etc.

We will also collect sensitive confidential data known as "special category personal data", in the form of health information, religious belief (if required in a healthcare setting) ethnicity and sex life information that are linked to your healthcare, we may also receive this information about you from other health providers or third parties.

Why do we need your information?

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 about you may include the following information;

- Details about you, such as your address, your carer or legal representative and emergency contact details.
- Any contact the surgery has had with you, such as appointments, clinic visits, emergency appointments.
- Notes and reports about your health.
- Details about your treatment and care.
- Results of investigations such as laboratory tests, x-rays etc.
- Relevant information from other health professionals, relatives or those who care for you.
- Contact details (including email address, mobile telephone number and home telephone number)

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. Limited information may be used within the GP practice for clinical audit to monitor the quality of the service we provided.

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 the course of 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 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

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.

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.

Medicines Management

The Practice 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.

GP Connect Service

The GP Connect service allows authorised clinical staff at NHS 111 to seamlessly access our practice's 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 with your GP Practice, 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 practice direct for an appointment.

The practice will not be sharing any of your data and the practice 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 your GP 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.

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

In light of the current emergency, 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 Additional Information. This change of requirement will be reviewed after the current coronavirus (COVID-19) pandemic.

Why we have made this change

In order 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:

1. **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.
2. **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.
3. **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 your GP practice or complete this form and return it to your GP practice.

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 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 your up to date details. 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 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

The Practice 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…'

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

The legal bases for processing this 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.

Categories of personal data

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).

Sources of the data

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.

Recipients of personal data

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).

Third party processors

In order to deliver the best possible service, the practice will share data (where required) with other NHS bodies such as other GP practices and hospitals. In addition, the practice 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.

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:

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

Every member of staff who works for an NHS organisation has a legal obligation to keep information about you confidential.

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 practice policy is to respect the privacy of our patients, their families and our staff and to maintain compliance with the General Data Protection Regulation (GDPR) and all UK specific Data Protection Requirements. Our policy is to ensure all personal data related to our patients will be protected.

All employees and sub-contractors engaged by our practice are asked to sign a confidentiality agreement. The practice will, if required, sign a separate confidentiality agreement if the client deems it necessary. If a sub-contractor acts as a data processor for Lime Grove Medical Centre Matlock 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. If some circumstances we may need to store your data after your consent has been withdrawn to comply with a legislative requirement.

Some of this information will be held centrally and used for statistical purposes. Where we do this, we take strict measures to ensure that individual patients cannot be identified. Sometimes your information may be requested to be used for research purposes – the surgery will always gain your consent before releasing the information for this purpose in an identifiable format. In some circumstances you can Opt-out of the surgery sharing any of your information for research purposes.

With your consent we would also like to use your information

There are times that we may want to use your information to contact you or offer you services, not directly about your healthcare, in these instances we will always gain your consent to contact you. We would however like to use your name, contact details and email address to inform you of other services that may benefit you. We will only do this with your consent. There may be occasions where authorised research facilities would like you to take part on innovations, research, improving services or identifying trends, you will be asked to opt into such programmes if you are happy to do so.

At any stage where we would like to use your data for anything other than the specified purposes and where there is no lawful requirement for us to share or process your data, we will ensure that you have the ability to consent and opt out prior to any data processing taking place.
This information is not shared with third parties or used for any marketing and you can unsubscribe at any time via phone, email or by informing the practice DPO as below.

National Opt-Out Facility

You can choose whether your confidential patient information is used for research and planning.

Who can use your confidential patient information for research and planning?

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

Making your data opt-out choice

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.

Will choosing this opt-out affect your care and treatment?

No, 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 screenings for bowel cancer.

What should you do next?

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 securely online or through a telephone service.

You can change your choice at any time. To find out more or to make your choice visit nhs.uk/your-nhs-data-matters or call 0300 303 5678

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

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.

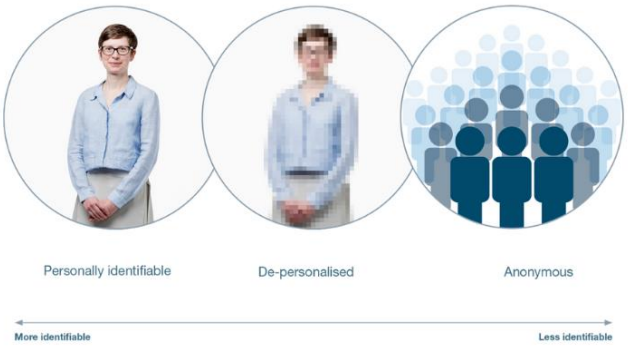

Image provided by Understanding Patient Data under licence.

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 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 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 below.

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.

The legal basis under UKGDPR for General Practice Data for Planning and Research

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. 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. More about the National Data Opt-out is in the section below.

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

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.

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 3rd 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.

Who are our partner organisations?

We may also have to share your information, subject to strict agreements on how it will be used, with the following organisations;

- NHS Trusts / Foundation Trusts
- GP's
- Primary Care Network
- NHS Commissioning Support Units
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers
- Ambulance Trusts
- Clinical Commissioning Groups
- Social Care Services
- NHS England (NHSE) and NHS Digital (NHSD)
- Multi Agency Safeguarding Hub (MASH)
- Local Authorities
- Education Services
- Fire and Rescue Services
- Police & Judicial Services
- Voluntary Sector Providers
- Private Sector Providers
- 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 consent for this to happen when this is required.

Computer System

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.

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 Lime Grove Medical Centre Matlock an appropriate contract (art 24-28) will be established for the processing of your information.

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.

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 (https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016).

How can you access, amend move the personal data that you have given to us?

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.

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.

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. The aim is that by July 2019, all areas within England will be 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 are expected to come together in geographical networks covering populations of approximately 30–50,000 patients by June 2019 if they are 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 the practice may share your information with other practices within the PCN to provide you with your care and treatment.

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 a project as a time limited pilot across named practices in Derby and Derbyshire.

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.

As part of this programme, personal data about your health care will have all identifiers removed (like your name or NHS Number) and replaced with a code which will be linked to information about care received in different health care settings. 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.

As part of this programme your GP and other care providers will send the information they hold on their systems to the North Of England Commissioning Support Unit (NECS). NECS are part of NHS England. More information can be found here https://www.necsu.nhs.uk

NECS 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. NECS work in partnership with a company called Optum to help them with this work. Both NECS and Optum are legally obliged to protect your information and maintain confidentiality in the same way that your GP or hospital provider is. More information about Optum can be found here www.optum.co.uk.

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.

The PHM project is time-limited to 22 weeks. Once the project has completed all de-identified , information processed by NECS / Optum will be securely destroyed. This will not affect any personal information held by your GP or other health or social care providers.

Access to your personal information

Data Subject Access Requests (DSAR): You have a right under the Data Protection legislation to request access to view or to obtain copies of what information the surgery 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. (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
- We are required to provide you with information within one month
- 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 information we hold about you at any time.

What should you do if your personal information changes?

You should tell us so that we can update our records please contact the Practice Manager 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), the practice will from time to time ask you to confirm that the information we currently hold is accurate and up-to-date.

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.

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.

Our website

The only website this Privacy Notice applies to is the Surgery's website. If you use a link to any other website from the Surgery'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.

The Surgery's website uses cookies. For more information on which cookies we use and how we use them, please see our Cookies Policy.

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.

Objections / Complaints

Should you have any concerns about how your information is managed at the GP, please contact the GP Practice Manager or the Data Protection Officer as above. If you are still unhappy following a review by the GP practice, 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 Practice 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 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

Changes:

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 Practice Data Protection Officer.

APPENDICES

1 DERBYSHIRE SHARED CARE RECORD

The Derbyshire Shared Care Record (DSCR) covers all persons accessing health and social care services in Derby and Derbyshire which equates to over 1 million citizens. The DSCR will contain personal information including demographic details, health and social care details. This therefore means that Special Category data (as defined by UK GDPR) will be processed and shared as part of the DSCR. The DSCR will contain information about all citizens (unless they object), including children.

The categories of information that will be shared are:

- Demographics
- Record summary
- Diagnoses
- Medication (current, past and allergies)
- Alerts and Hazards
- Procedures
- Investigations
- Encounters, admissions and referrals
- Letters from Hospitals and other Health and Care Professionals

Specific datasets for each organisation or system will be defined as part of the project. Approval from each Data Controller is required before any information is shared from their system(s). Some datasets/systems will provide a live 'view' of the record, and other systems will require data to be extracted and stored securely on an encrypted server.

Purpose of Information sharing

The goal of the DSCR is to enable information sharing between health and social care organisations in Derbyshire for the purposes of delivering direct care. The purpose of the DSCR is:

- To support the delivery of integrated health and social care to people in Derbyshire
- To enable health and social care professionals working across all Derbyshire and Derby city's NHS and local authority social care organisations to have wider access to records to support their care of individual patients
- To enable health and social care professionals working across all Derbyshire and Derby to make informed decisions
- To support the delivery of urgent care and safeguarding services across all the partners, where access to up-to-date, multi-agency information reduces the risk of avoidable harm to the individual(s)
- To enable clinicians and social care practitioners to more readily establish which other agencies are involved with a person, to gather key information to enable them to care for people more safely and efficiently, without referring to multiple records systems, or using alternative time consuming and labour intensive communication methods such as telephone

Basis for information sharing

All health and adult social care providers are subject to the statutory duty under section 251B of the **Health and Social Care Act 2012** to share information about a patient for their direct care. This duty is subject to the common law duty of confidence, the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR).

It is important that all professionals discuss information sharing with citizens so that they are aware of how their information is accessed and shared by those involved in their care.

UK GDPR

Under UK GDPR there must be a valid lawful basis to process personal data. For UK GDPR sharing information for the DSCR is on the basis of public task where "processing is necessary for the

performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"
Article 6(1)(e) of the UK GDPR is the condition for lawfully processing data for delivering direct care as part of the DSCR:
6(1) (e) '…for the performance of a task carried out in the public interest or in the exercise of official authority…'
Article 9(2)(h) of the GDPR is the condition for processing 'data concerning health' (personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status) for direct care as part of the DSCR:
9(2) (h) '…medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'
Safeguarding
There are legal provisions that support the release of data for the purposes of safeguarding children and vulnerable adults. The Children Acts 1989 and 2004 establishes implied powers for local authorities to share information to safeguard children, safeguard and promote the welfare of children within their area who are in need, and to request help from specified authorities including NHS organisations. The Care Act 2014 sets out a legal framework for how local authorities and other parts of the health and social care system should protect adults at risk of abuse or neglect.
For UK GDPR, in addition to the Articles 6(1)(e) and Article 9(2)(h) cited above, there is an additional provision for sharing data for the purposes of safeguarding, as follows:
9(2)(b) …'is necessary for the purposes of carrying out the obligations and exercising the specific rights of the controller or of the data subject in the field of…social protection law in so far as it is authorised by Union or Member State Law …'
Informing Citizens
A public awareness campaign will take place to ensure the DSCR is complying the UK GDPR 'Right to be Informed' (articles 13 and 14).
A full communications and engagement strategy has been developed to ensure there is a robust campaign which uses a range of different communication media and providing accessible information. Communications will clearly explain the benefits and purpose of DSCR, including the organisations that their information may be shared with, plus details of how citizens can object from having a shared care record should they wish to opt out.
A privacy officer will be in place to be a single point of contact for queries from citizens about the DSCR. The privacy officer will be able to advise citizens, process requests to opt out or opt back in, and also manage any requests for audit trails of record access. The Privacy Officer will have a list of Data Protection Officer contact details for all partners and ensure that any relevant privacy issues are promptly referred to the relevant partner where appropriate, in accordance with this agreement.

5. Exchange of information
Dependent on the source system, information will either be shared as a live 'view' (using an API) from the source system or extracted overnight and viewed from within the Orion Health data warehouse.
Appendix 1 summarises the method and categories of information exchange from the different systems in scope (as at May 2021).
No data will be shared in to the DSCR without approval from the data controller of that information.
6 Terms of use of the information
The DSCR partner organisations and signatories of this agreement are the joint data controllers of the DSCR. This means they share joint responsibility for the use and manner in which DSCR data is processed. The partner organisations remain individually responsible for the data that is held in their own systems.

Two suppliers responsible for delivering parts of the DSCR are Orion Health Limited (Data Processor) and NextGate (Sub-processor contracted through Orion Health, who manage the master patient index). These suppliers are responsible for processing (e.g. storing, retrieving and linking) data on behalf of the data controllers. They do not have any responsibility or control over DSCR data. Orion Health use Amazon Web Services (AWS) to store any extracted patient information for the DSCR.

7. Data Protection Impact Assessments

Under the UK General Data Protection Regulations, a Data Protection Impact Assessment (DPIA), which is an assessment made prior to processing of the impact of the processing on the protection of personal data, will be mandatory in certain circumstances. This will be the case where the processing is likely to result in a high risk to the rights and freedoms of individuals. Therefore, all parties will ensure in these circumstances that they complete a data protection impact assessment so that they can assess the risks to individuals and take steps to mitigate against those risks.

8. Data quality assurance

The DSCR receives information (see section 5 for the methods of exchange) from source systems and therefore any identified data quality issues should be corrected in the appropriate source system. Users should notify the originating organisation (the data controller) of the information in order for any data quality issues to be investigated and amended as appropriate.

In some cases, the system administrators will investigate issues and, if the issue relates to the way the information has been processed by the DSCR, the Orion Health process will be followed to report and correct the issue.

8. Data retention, review and disposal

The DSCR does not change the length of time that data will be kept for. Data will be retained in partner source systems for time periods that are compliant with data protection legislation. Each Partner will maintain a retention schedule based on industry best practice and statutory retention periods such as the Records Management Code of Practice for Health and Social Care 2016, the Limitation Act 1980, the Local Government Association Guidance.

Joined Up Care Derbyshire have determined that care of individuals is enhanced by the sharing of information with appropriate safeguards. This also links to the Caldicott Principle – "the duty to share information is as important as the duty to protect confidentiality".

If a partner to this ISA wishes to withdraw from feeding information to the DSCR, they can stop the feed. In the case of GP records, with a live view of information, no data will reside on the shared record. For other agencies, the partners would work with Orion Health to establish how to deal with records previously uploaded to DSCR. Information held in the DSCR may have been used to inform a clinical decision and so rather than being deleted, information will normally be restricted from view.

9. Access and security

Orion Health have ISO/IEC 27001:2013 accreditation. Orion Health documentation is available to ISA partners on request, including the Orion Health Global Information Security Management System (ISMS).

Both information held by Orion Health and any information transfers comply with the encryption standard AES 256.

Information will be viewed by approved users through the Orion Health DSCR Portal. Wherever possible, Single Sign-On (SSO) will be enabled so that staff search for a patient within their own electronic record system and then click through to view the same patient's record within the DSCR. In systems or environments where SSO is not possible, users will log in to the portal using their own username and password and will be able to search for records using primary identifiers such as the NHS Number.

Staff will need to be approved for access to the DSCR and a full Role Based Access Control (RBAC) model will be in place. All access will be tracked and auditable. All staff will have received training on how to use the DSCR, and their responsibilities, before being given access.

No part of the system is accessible without a username and password, each user must also be registered to at least one Access Group, which determines the level of functionality they can access, as defined by the RBAC model.
To prevent unauthorised access, users are automatically logged out following a configurable period of inactivity. If the user is at a workstation, they are prompted to prevent the logout before it occurs.
Organisations are responsible for ensuring that all staff have completed annual Information Governance / Data Protection training in line with Data Security and Protection Toolkit requirements.
Each party must make sure that they have procedures in place to do everything reasonable to:
• make accidental compromise or damage unlikely during storage, handling, use, processing transmission or transport.
• deter deliberate compromise or opportunist attack.
• dispose of or destroy the data in a way that makes reconstruction unlikely.
• promote discretion to avoid unauthorised access.
• be ready and prepared to respond to any breach of security swiftly and effectively and all parties must ensure that any breaches are reported to the data controller within one working day.
• comply with the deadline for reporting a breach to the relevant data controller.
• maintain a record of personal data and processing activities regarding the data.
• ensure that access to information subject to this agreement will only be granted to those professionals who 'need to know' to effectively discharge their duties.
• have policies and systems in place to ensure information held on its information systems is held securely and in compliance with industry security standards and legislation.

10. Breaches of Confidentiality
All activity on the DSCR is logged in an audit trail, and the individual user is responsible for justifying why they looked at a specific record.
Under Article 33 of UK GDPR, breaches that must be reported to the Information Commissioner's Office (ICO) are defined as a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
These breaches should be reported to the ICO without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. The Data Protection Officer (DPO) of the organisation detecting the breach should be informed, and they will inform the DSCR Privacy Officer. Other IG leads, as appropriate, will be advised of the breach by either the detecting organisation or the Privacy Officer within 24 hours whenever possible.
Any organisation either suspecting or identifying inappropriate use by their own staff will conduct their own investigation. If this identifies that information from another organisation has been viewed or used inappropriately, the original organisation will contact the relevant IG Lead. Organisations will then follow their own incident management and Disciplinary procedures as appropriate.
Any organisation either suspecting or identifying inappropriate use by users outside of their employees will raise the issue as soon as possible with the DPO for the organisation responsible for those users.
11. Data Protection Rights
Each Party will comply with the statutory data protection rights, namely:
• Transparency of Communication
• Right of access
• Right to be informed
• Right to rectification

- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights in relation to automated decision making and profiling

Requests will be referred to the relevant party, and/or the privacy officer will refer rights requests to the relevant data controller as soon as possible, within two working days.

12. Management of the Agreement

This ISA will be reviewed on 1st August 2022 or sooner if requested by any of the partners to the ISA. Any requests by external parties, including Freedom of Information requests, for copies of the ISA or other documentation relating to the DSCR should be directed to the Privacy Officer at crhft.enquiries.DSCR@nhs.net

Field CodeChanged

2 ENHANCED DATA SHARING MODULE – SYSTMONE (GP COMPUTER SYSTEM)

Systmone stores your health information records.

These records store important and often sensitive, confidential, information about your illnesses and the care you have received in the past. Your record may contain contributions from various health and social care organisations, especially if your needs are complex. These may include records from urgent care settings to the physiotherapy service you may have attended.

Organisations can access your medical record if you give them permission. This is likely to benefit the care you receive. You may choose to decline to have your information shared in this way but this could disrupt your care. You may also change your mind about sharing at any time. Organisations using SystmOne should only access your record when they are involved in giving you care.

We aim to ensure that your choices about how your information is shared are respected.

We will ask you to give us your preferred mobile phone number or email address which will be recorded on your medical record. This means that when another organisation asks to access your record, we can send you a verification (security) code which allows you to choose whether to let that organisation access your medical record or not.

For example you may be working or on holiday in another part of the country and need care from a hospital, or clinic. Having access to your whole medical record will benefit the care they can provide you. It may allow for better care provision if healthcare workers can access your full medical record.

If you already use the SystmOnline patient portal, then you can select organisations to allow or prevent them from accessing your records,

If you do not have a phone or email address and don't use SystmOnline, then your GP practice will be able to record your choices about which organisations you are happy to share your whole record with.

When you receive care close to your home you will not usually need to give a verification (security) code but you should always still be asked what your choices are about record sharing.

If you would like to read more about SystmOnline, and these new sharing controls, please go to https://systmonline.tpp-uk.com/2/help/help.html or ask at your GP practice.

3 MIG – MEDICAL INTEROPERABILTY GATEWAY DERBYSHIRE

This project is part of a wider programme to develop integrated digital care records for approximately 1,100,000 patients in Derbyshire.

The Medical Interoperability Gateway (MIG) is 'middle-ware' technology that allows Local Health and Care economies (excluding Primary Care, at present) to view identifiable patient GP data in 'real-time' utilising 'implied consent to share' and 'explicit consent to view' model. I.e. a clinician will ask the patient at the point of care for 'permission to view' their GP patient record; however this can be overridden when in the vital interests of the patient i.e. in a life and death situation.

The MIG provides a 'view' of a specified data set from the Primary Care Record, with no data moving from the system from the GP record to the 'viewing' system and no data is transferred back into a GP record.

In essence, the MIG allows viewing of GP clinical data in clinical settings outside the patient's GP Practice, supporting health and care professionals to make a more informed clinical decision. GP records can be explicitly marked as private, for example sensitive records, if necessary. Sexual Health, HIV and other sensitive data items, such as Termination of Pregnancy (TOPs) have been excluded in line with Healthcare Gateway's MIG Content Model Record for EMIS practices only. TPP SystmOne have not implemented this model and expect GPs to discuss marking these and other parts of the

record as private. This will be communicated to GPs to ensure they are aware and can appropriately inform patients.

Details of patients who have dissented from sharing would not be available to view via the MIG. These activities/consents are managed by the patient's registered GP Practice whenever one of their patients requests their sharing wishes to be recorded. Should a patient dissent from sharing the patient's practice would record this wish on the patient's GP record. This recording would have an associated clinical code that ensures the patient's data is not made available to view via the MIG.
Where a patient has already raised a Type 1 objection for identifiable information to be shared outside of the GP Practice, the code to dissent would have been applied to the patient's record therefore these patient's records will not be available through the MIG.

Patient information made available from GP system via MIG for direct patient
care can be viewed by clinicians and social care professionals with a legitimate relationship with the individual patient.

The data available to view is a selective dataset from a patient's medical record of the following 10 areas:

Data Available to View via MIG:

- Summary
- Problems (current and past)
- Current and Past Diagnosis
- Current, Past Medication and Medication Issues
- Risk and Warnings (Allergy and Contraindications)
- Procedures (Operations, Vaccination/Immunisations)
- Investigations
- Examinations (Blood pressures)
- Events (Encounters, Referrals and Admissions)
- Demographics
- End of Life dataset

The information accessed is to support Health and Social Care professionals to make informed decisions during consultations with the patients when a patient presents to a health or care setting outside of their registered GP Practice. Access to the data is in 'real-time' and via the consent to view model, however this can be overridden when in the vital interests of the patient i.e. in a life and death situation.
Patient information is made available from GP systems via the MIG for direct patient care provided by Health and Careprofessionals with a legitimate relationship with the individual patient.
When the professional accesses the clinical data available to them via the MIG (see table above) this would provide a supportive and positive impact on the patient. The clinician should be able to make a more informed decision about the patient particularly in an emergency and urgent care setting and could result in timely and informed follow-on referrals and treatment in support of delivering direct care to the patient
Patient Safety
- Increased patient safety with information available at the point of care
  - Allergies & Adverse Reactions
  - Current medication
  - Dynamic diagnostic

- Tests Results
- Significant History
- Operative Procedures
- Latest Examinations
- Events – Referrals, Admissions etc.
- Vaccinations and Immunisations

Patient Empowerment/Experience

- An improved patient experience through effective sharing of key patient information with the specialist delivering care
- Satisfied patient and staff improvement in the timely communication between key care professionals and organisations
- Patients no longer having to repeat details of their history to multiple health and care settings

Quality of Patient Care

- Improvements in the recording and presentation of the information necessary:
  - To support avoidance of unnecessary admissions
  - To support avoidance of ED attendances
  - To avoid unnecessary diagnostic testing
  - To avoid inappropriate conveyance of a patient to hospital

Empowering Health Professionals

- Provision of data – the Information shared is detailed and up to date
- Treating the patients with full confidence of aspects of health and care history
- Efficiency & Effectiveness
- Immediate time savings – with reduced calls to practices to gather information allowing staff to focus on other areas of service delivery
- Reduction in calls to Health and Care allows staff to focus on other areas of service delivery
- Fully integrated with accredited systems (remaining systems to follow) – no need to log into multiple systems