Well Street Medical Centre (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 that we may collect from or about you.

This privacy notice applies to personal information processed by or on behalf of Well Street Medical Centre.

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 process
- The legal grounds for our processing of your personal information (including when we share it with others)
- What to do if your personal information changes
- For how long your personal information is retained by us
- Your rights under data protection laws

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA18) became law on 25th May 2018. The GDPR is a single EU-wide regulation on the protection of confidential and sensitive information and the DPA18 implements the regulations into comprehensive UK legislation. Following the decision for the UK to leave the European Union and the end of the transition period, from 1st January 2021 the UK has been subject to an Adequacy Agreement which will allow data to continue to be shared with European Union Countries without further safeguarding being necessary. This is to allow the European Commission suitable time to grant the UK with adequacy status, meaning they have met the required standards in ensuring data transfers to and from the UK are safe.

For the purpose of applicable data protection legislation the practice responsible for your personal data, and referred to as the Data Controller, is ***Well Street Medical Centre***.

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

Well Street Medical Centre will be what's known as the ' Data Controller' of the personal data you provide to us.

We collect basic personal data about you which includes name, address, contact details, date of birth and next of kin information 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. 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, on paper or a mixture of both, and we use a combination of working practices and technology to ensure that your information is kept confidential and secure. Records which the Practice holds about you may include the following information;

- Details about you, such as your contact details, your carer or legal representative and emergency contact details
- Any contact the surgery has had with you, such as appointments, telephone calls, clinic visits and emergency appointments.
- Notes and reports about your health
- Details about your treatment and care
- Results of investigations such as laboratory tests (e.g. urine and blood results) and imaging reports (e.g. x-ray and ultrasound)
- Relevant information from other health professionals, relatives or those who care for you

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

How do we lawfully use your data?

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

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 a number of 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, so being far more proactive in an ever-changing health climate. As a result of risk stratification, your GP may be able to offer you additional services.

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.

Our data processor for Risk Stratification is: Midlands and Lancashire Commissioning Support Unit (CSU)

Facilitation of Admission Avoidance Scheme Agreement
The Practice participates in a local improvement scheme and receives funding from Staffordshire and Stoke-On-Trent Clinical Commissioning Group (CCG) to proactively case manage a selected cohort of patients deemed most at risk of unexpected hospital admission. The scheme's focus is to reduce attendances at emergency portals and non-elective admissions in its most vulnerable cohort. To enable the impact of the scheme to be quantified, data is uploaded from the practice through to NHS Digital's Data Services for Commissioners Regional Office (DSCRO), hosted by Midlands & Lancashire Commissioning Support Unit, to allow the number of non-elective admissions to be monitored during the life of the scheme. On a monthly basis the practice uploads the NHS numbers of all patients receiving care under the scheme with the date of their last care review. No other patient identifiable data leaves the practice. The NHS number is then pseudonymised and provided to the Midlands & Lancashire Commissioning Support Unit Data Warehouse team. The team utilise the pseudonymised identifier to provide a report showing emergency attendance and admission activity pre and post intervention via the scheme. Staffordshire and Stoke-On-Trent Clinical Commissioning Group (CCG) utilise this report to measure the impact of the scheme and create a case for continued funding. Please note that you have the right to opt out of this data extraction. A copy of the full data sharing agreement between the parties is available online and can be printed on request.

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 (led by quality, safety or efficiency) are carried out by the Clinical Commissioning Group's Medicines Management Team under a Data Processing contract with the Practice. Reviews collect key patient demographics and medication details to enable the Practice clinical team to identify improvements and optimise patient care.

Datix Reporting
Staffordshire and Stoke-On-Trent Clinical Commissioning Group (CCG) utilise a web-based system to collate feedback on healthcare providers called Datix. The Practice enters details of patient feedback, adverse incidents and complaints to allow the CCG to follow up reported events and identify wider themes and trends. When reporting individual events, the Practice records the patient NHS number. This supports Providers to review episodes of care, provide relevant feedback and identify areas for improvement.

Data entered into Datix is stored securely and is password controlled with role based access. Data is only shared with commissioned Provider organisations to support the consideration of items for Soft Intelligence; it is not used in any other way.

Extended Access Service Hubs
Extended access service hubs (operated by North Staffordshire GP Federation) offer patients, registered at practices in North Staffordshire, access to GP and Nurse appointments on weekday evenings and at weekends. Clinicians working within the hubs will have access to patient records via the EMIS EPR viewer. Following an appointment being booked with the service, data will be shared between the Practice and the service hub. This will include demographic information and the patient clinical record. Reception staff at the service hubs will have role-based access and will not see medical details. Data will be shared for an individual patient each time they have an appointment with a service hub. A summary of the consultation at the service hub will be electronically sent to the practice and retained within the GP patient record. This data sharing between the Practice and the extended access service hubs enables safer, more informed and better quality care. A copy of the full data sharing agreement between the parties is available online and can be printed on request.

GP connect service

The GP Connect service allows authorised clinical staff such as GPs, NHS 111 Clinicians, Care Home Nurses (if you are in a Care Home), Secondary Care Trusts and Social Care Clinicians to access the GP records of the patients they are treating via a secure NHS Digital service called GP Connect. This is to support direct patient care. The service also supports organisations such as NHS 111 to directly book GP appointments.

One Health & Social Care (OHC) Shared Record
One Health and Care is a confidential shared care record which brings data together from the different organisations involved in your health and social care. It allows doctors, nurses and other registered health and social care professionals directly involved in your care to view relevant information in order to provide you with better, safer care. To view the full list of participating organisations in primary, secondary and community care, understand what data will be shared and how, along with your rights in relation to this processing, please view the full One Health & Social Care privacy notice: https://staffsstokeics.org.uk/your-health-and-care/shared-health-and-care-record/one-health-and-care-privacy-notice/#:~:text=One%20Health%20and%20Care%20allows%20your%20data%20to,to%20appropriate%20standards%20of%20privacy%2C%20security%20and%20transparency. Patients who have recorded a Type 1 objection with the Practice will not have a shared care record.

Patient Communication
The Practice will use your name, contact details and email address to inform you of NHS services, or to provide information to manage your healthcare. There may be occasions where authorised research facilities would like you to take part in research in regard to your particular health issues, to try and improve your health. Your contact details may be used to invite you to receive further information about such research opportunities, but you must give your explicit consent to receive messages for research purposes.

Telephone System and Call Recording
Well Street Medical Centre has an advanced telephony system, Surgery Connect, which is capable of recording conversations. All calls (inbound and outbound) are recorded for training and monitoring purposes.

Whilst recordings will not routinely be accessed, they may assist in:

- Protecting the interests of both parties on the call, including protecting Practice staff from nuisance or abusive calls.
- Investigating complaints and establishing facts.
- Aiding standards in call handling through use in training and coaching (providing the identity of the patient is anonymised).

Well Street Medical Centre will make every reasonable effort to advise callers that their call may be recorded and for what purpose recordings may be used. This will normally be via a pre-recorded message within the telephone system.

Audio recordings are stored within the Surgery Connect platform. Surgery Connect are an NHSX framework approved supplier who have demonstrated their compliance with rigorous NHS security standards. The recordings are only accessible through Practice devices and require high level access rights, held only by the Practice Management team. Any playback of recordings will take place in a private setting.

Audio recordings fall under the scope of personal data. Requests for copies of audio recordings can be made as a Subject Access Request (SAR). This should be made in writing, and after assessing if the data can be released, the requester can be invited to the Practice premises to hear the recording or a transcript can be provided.

Recorded data is retained for 36 months. You have the right to object to your telephone call being recorded. Please raise your objection to recording at the start of any call, in order for the call handler to stop further recording.

Primary Care Networks
The objective of Primary Care Networks (PCNs) is for group practices working together to create more collaborative workforces which ease the pressure on GP's, leaving them better able to focus on patient care. The aim is for all areas within England to 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 and take advantage of additional funding attached to the GP contract.

This means the practice may share your information with other practices within the Moorlands Rural PCN (Allen Street Surgery, Alton Surgery, Tardis Surgery, Tean Surgery, Waterhouses Surgery and Werrington Surgery) to provide you with your care and treatment.

Additional Roles Reimbursement Scheme (ARRS) Mental Health Practitioners Service for utilisation across Staffordshire Primary Care Networks (PCNs) – Data Extraction and Reporting

Mental Health Practitioners (MHPs) work across PCNs in Practice settings to deliver mental health services, with the aim of preventing or reducing the need for more specialised services. Whilst working on behalf of Practices, MHPs are employed by North Staffordshire Combined Healthcare NHS Trust (NSCHT). To monitor the efficacy of the service provided, limited, anonymised data will be shared with NSCHT on a monthly basis on activity and outcomes to better develop future interventions and shape onward service provision.

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.

Categories of personal data
The data collected by Practice staff in the event of a safeguarding situation will be sufficient personal information to inform staff, assess risk and enable investigation where appropriate. In addition to basic demographic and contact details, we will also process details of what the safeguarding concern is. This is likely to be special category 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.

Sharing information
We may share information with other partners such as local authorities, the police or healthcare professionals to meet our duty of care and enable investigation.

Child Health – Vaccinations and Immunisations
Management of child and school-aged immunisations is locally contracted to the Staffordshire and Stoke-On-Trent Health Informatics Service. The Child Health Immunisation team schedule vaccinations and immunisations in line with the national immunisation programme to ensure patients are offered vaccination at the most effective times, and monitor subsequent uptake. The team have access to demographic, registration and vaccination history details. Data is shared between the Practice and the Health Informatics Service through a data processor: Health Intelligence Ltd. A copy of the full data sharing

agreement between the parties is available online and can be printed on request.

General Practice Data for Planning and Research

Note: The Government is delaying the implementation of the General Practice Data for Planning and Research (GP DPR) programme until four key areas of work are strengthened:

This Privacy Notice will be updated when further details of the proposed implementation have been confirmed, and this may not be for at least another 12 months.

For further information please refer to NHS Digitals webpage on this subject matter *

The NHS needs data about the patients it treats in order 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. We have agreed to share the patient data we look after in our practice with NHS Digital who will securely store, 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

This means that we can get on with looking after our 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 is engaging 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.

Opting Out

If you don't want your identifiable patient data to be shared for purposes except for your own care, you can opt-out by registering a Type 1 Opt-out or a National Data Opt-out, or both. These opt-outs are different, and they are explained in more detail below. Your individual care will not be affected if you opt out using either option.

Type 1 Opt-Outs - If you do not want your identifiable patient data to be shared outside of the GP practice for purposes except your own care, you can register an opt-out with the 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, patients who have registered a Type 1 Opt-out will be informed. There is more information about National Data Opt-outs below.

NHS Digital will not collect any patient data for patients who have already registered a Type 1 Opt-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 for the purposes above, 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.

If you have already registered a Type 1 Opt-out with us your data will not be shared with NHS Digital. If you wish to register a Type 1 Opt-out with us before data sharing starts with NHS Digital, this should be done by returning this form to the practice. If you do intend to opt out of the GP DPR we will update this Privacy Notice with the date by which you must provide your opt-out by to allow time for processing it. 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 return the form to the Practice. Call **0300 3035678** to request a form be sent out to you.

If you do not want NHS Digital to share your identifiable patient data with anyone else for purposes beyond your own care, then you can also register a National Data Opt-out.

National Data Opt-Out

If you don't want your confidential patient information to be shared by NHS Digital with other organisations for purposes except your own care - either GP data, or other data it holds, such as hospital data - you can register a National Data Opt-out.

If you have registered a National Data Opt-out, NHS Digital will not share any confidential patient information about you with other organisations, unless there is an exemption to this, such as where there is a legal requirement or where it is in the public interest to do so, such as helping to manage contagious diseases like coronavirus. You can find out more about exemptions on the NHS website.

There is an intention for the National Data Opt-out to apply to any confidential patient information shared by the GP practice with other organisations for purposes except your individual care. This means it will replace the Type-1 Opt-out. If this happens, patients who have registered a Type 1 Opt-out will be informed. Please note that the National Data Opt-out will not apply to confidential patient information being shared by GP practices with NHS Digital, as it is a legal requirement for us to share this data with NHS Digital and the National Data Opt-out does not apply where there is a legal requirement to share data.

You can find out more about and register a National Data Opt-out or change your choice on nhs.uk/your-nhs-data-matters or by calling **0300 3035678.**

You can also set your opt-out preferences via the NHS App if you are registered to use this application. Well Street Medical Centre is compliant with the National Data Opt-Out.

The legal bases for processing this information
The Health and Social Care Act 2012 covers the sharing and collection of health and care data. It says that when the Secretary of State for Health and Social Care needs to collect and analyse data to help the health service, they can tell NHS Digital to do this for them. The instruction, which NHS Digital must act on, is called a **direction**. In this case:

1.) The Secretary of State for Health and Social Care sent a direction to NHS Digital, instructing them to collect and analyse general practice data for health and social care purposes including policy, planning, commissioning, public health, and research purposes.

2.) NHS Digital sent all GP practices a document called a Data Provision Notice, giving details of the data it needs GP Practices like ours to share so it can comply with the direction. All GP Practices in England are required to share data with NHS Digital when they are sent a Data Provision Notice.

Under data protection law, we can only share patient data if we have a legal basis under Articles 6 and 9 of the UK GDPR. Our legal basis for sharing patient data with NHS Digital is **Article 6(1)(c) - legal obligation, as we are required under the 2012 Act to share it with NHS Digital.**

When we are sharing patient data about health, we also need a legal basis under Article 9 of the UK GDPR. This is:

- **Article 9(2)(g)** – as we are sharing patient data for reasons of substantial public interest, for the purposes of NHS Digital exercising its statutory functions under the General Practice Data for Planning and Research Directions. It is substantially in the public interest to process patient data for planning and research purposes to improve health and care services for everyone. This is permitted under paragraph 6 of Schedule 1 of the Data Protection Act 2018 (DPA).
- **Article 9(2)(h)** – as we are sharing patient data for the purposes of providing care and managing health and social care systems and services. This is permitted under paragraph 2 of Schedule 1 of the DPA.
- **Article 9(2)(i)** - as patient data will also be used for public health purposes. This is permitted under paragraphs 3 of Schedule 1 of the DPA.
- **Article 9(2)(j)** - as patient data will also be used for the purposes of scientific research and for statistical purposes. This is permitted under paragraph 4 of Schedule 1 of the DPA.

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 data hosting service providers.

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

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 UK General Data Protection Regulations (GDPR) and 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 Well Street Medical Centre an appropriate contract 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 Practice Manager, Jessica Harding, 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.

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 to:

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.

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, such as a Data Processing Agreement, have been put in place. 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.

TPP SystmOne

The Practice uses a clinical system provided by a Data Processor called TPP SystmOne.

The system is a secure centralised system which supports modules for every healthcare setting from primary care to hospitals, social care and mental health. SystmOne provides clinicians and health professionals with a single shared Electronic Health Record (EHR) available in real time at the point of care.

The data will remain in the UK at all times and allows patient data to be shared securely across services—promoting efficiency and standardisation. Most importantly it enables services to improve the patient experience and deliver safer patient care.

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
- GPs
- Primary Care Networks
- North Staffordshire GP Federation
- 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)
- Local Authorities
- Multi agency Safeguarding Hub (MASH)
- Safeguarding Teams
- Education Services
- Police & Judicial 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 consent for this to happen when this is required.

Summary Care Record

All patients registered with a GP have a Summary Care Record (SCR), unless they have chosen not to have one. During the height of the pandemic changes were made to the SCR to make additional patient information available to all appropriate clinicians when and where they needed it, to support direct patient care, leading to improvements in both care and outcomes. These changes will remain in place.

Your SCR will contain details of your medication, allergies and adverse reactions, significant medical history (past and present), reasons for medications, care plan information and immunisations. You can choose to limit your SCR to medication, allergies and adverse reactions or you can choose to opt out of having an SCR all together but 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 change or check your preference, please speak to our team.

Shared Care Records

To support your care and improve the sharing of relevant information to our partner organisations 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.

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://www.nhsx.nhs.uk/media/documents/NHSX_Records_Management_Code_of_Practice_2020_3.pdf

Destruction
This will only happen following a review of the information at the end of its retention period. Where data has been identified for disposal, we have the following responsibilities:

- To ensure that information held in manual form is destroyed using a reputable confidential waste company (Shred-It) that complies with European Standard EN15713 and obtain certificates of destruction.
- To ensure that electronic storage media used to store or process information are destroyed or overwritten to national standards.

What are your rights over your personal data?

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. You have the following rights in relation to your data:

Right to rectify: The review, and where appropriate, correction of personal data when believed to be incorrect, out of date or incomplete will be acted upon within one calendar month of receipt of such a request.

Right to be informed: You have the right to be informed on how we handle, process and share your personal information; this privacy notice ensures as a Practice we satisfy this right.

Right to object: If we are using your data because we deem it necessary for our legitimate interests to do so, and you do not agree, you have the right to object. We will respond to your request within 30 days (although we may be allowed to extend this period in certain cases). Generally, we will only disagree with you if certain limited conditions apply. If we didn't process any information about you and your health care it would be very difficult for us to care and treat you.

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 market to you, you may withdraw your consent at any time.

Right to erasure: Under Article 17 of the GDPR individuals have the right to have personal data erased. This is also known as the 'right to be forgotten'. The right is not absolute and only applies in certain circumstances, for example when your personal data is no longer necessary for the purpose which it was originally collected or processed it for of if you wish to withdraw your consent after you have previously given your consent.

Right to restrict processing: Article 18 of the GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that you can limit the way that the practice uses your data. This is an alternative to requesting the erasure of your data. Individuals have the right to restrict the processing of their personal data where they have a particular reason for wanting the restriction.

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.

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.

- Your request should be made to the Practice – for information from the hospital or other NHS organisation you should write directly to them
- There is no charge to have a copy of the information held about you (charges do apply in the case of duplicate or excessive requests)
- We are required to respond to you within one calendar month
- You will need to give adequate information (for example full name, address, date of birth, NHS number and details of your request) and/or show proof of identity in order for your identity to be verified and your records located.

On processing a request, there may be occasions when information may be withheld if the organisation believes that releasing the information to you could cause serious harm to your physical or mental health. Information may also be withheld if another person (i.e. third party) is identified in the record, and they do not want their information disclosed to you.

What should you do if your personal information changes?

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

Objections / Complaints

Should you have any concerns about how your information is managed by our Practice, please contact Practice Manager, Jessica Harding or our Data Protection Officer (details below). If you are still unhappy following a review by either party, 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 extracted and 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 Practice Manager, Jessica Harding or our Data Protection Officer: Hayley Gidman, Head of Information Governance at Midlands and Lancashire Commissioning Support Unit.

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's Data Protection Officer is Hayley Gidman, Head of Information Governance at Midlands and Lancashire Commissioning Support Unit (CSU):

Email:	hayley.gidman@nhs.net
Telephone:	01782 872 648
Postal:	Midlands and Lancashire CSU Heron House 120 Grove Road Stoke on Trent ST4 4LX

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 Practice Manager, Jessica Harding or our Data Protection Officer: Hayley Gidman, Head of Information Governance at Midlands and Lancashire CSU.

Useful Links

Please find below some links to external webpages which you may wish to access to find out additional information:

- Information Commissioners Office
- Information Governance Alliance
- NHS Constitution
- NHS Digital Guide to Confidentiality in Health and Social Care
- Health Research Authority
- Health Research Authority Confidentiality Advisory Group (CAG)
- National Data Opt-Out