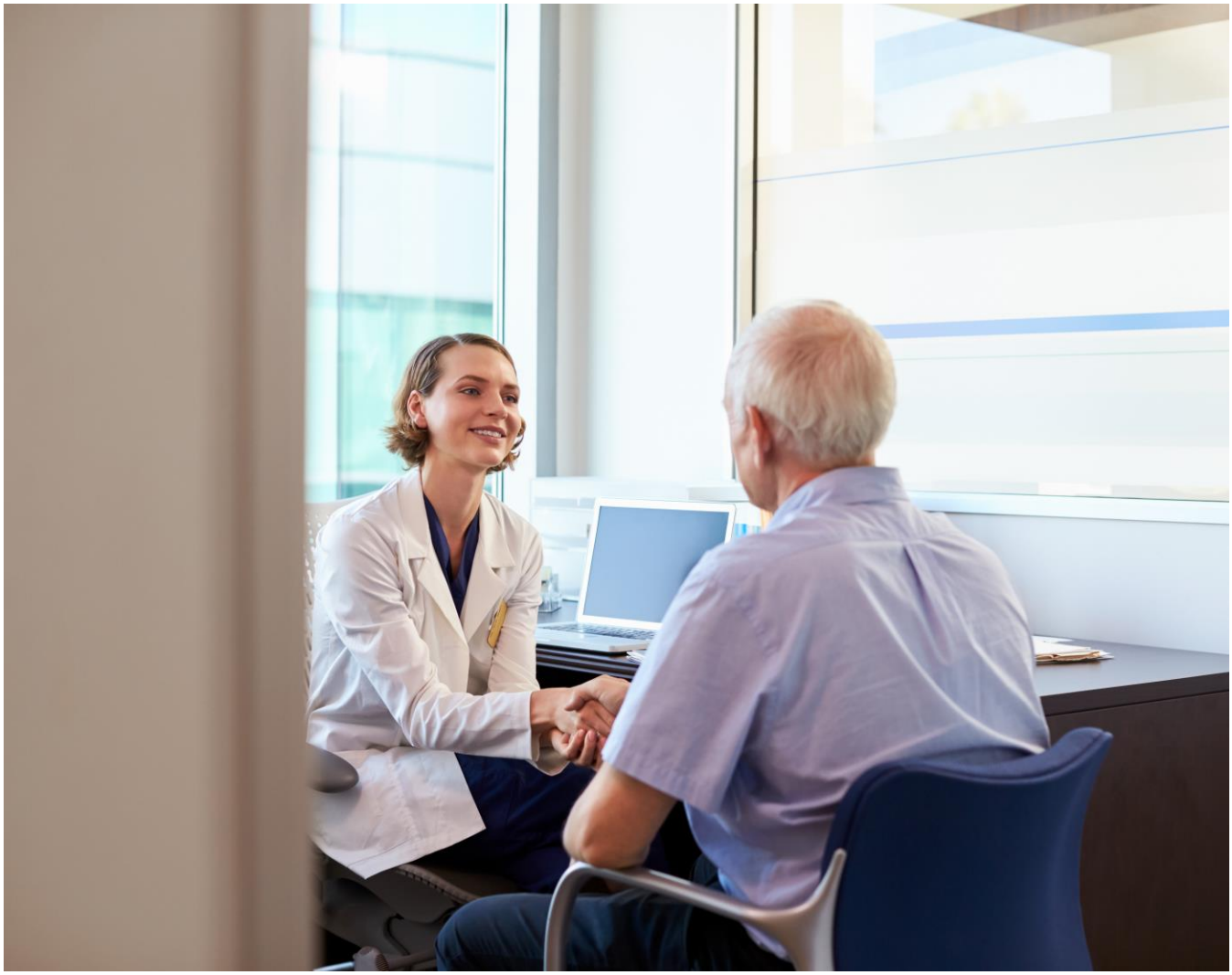
Practice Privacy Notice

Last updated: 19th August 2022 v2.6

This is a comprehensive overview on how your personal information is used by our General Practice, the NHS and our healthcare partner organisations. Please feel free to ask a member of staff for separate leaflets on specific data privacy topics such as our 'Data Privacy Guidance for Children'. Our full contact details are included at the end of this document.



Contents

How do we use your personal data?

Personal data is any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

What types of personal data are used by our General Practice?

An example of information we use that constitutes personal data includes:

- Your name, address, telephone numbers, an email address and an identification number (e.g. every patient has a unique NHS ID Number)
- We may hold details on other people such as your carer, legal representative or emergency contacts
- Any contact the surgery has had with you - such as appointments, clinic visits, emergency appointments
- Notes and reports about your health and details about your treatment and care
- Results of investigations such as laboratory tests or x-rays etc.
- Relevant information from other health professionals, relatives or those who care for you
- An online identifier on a website (e.g. website 'cookies' that track) - reflecting changes in internet technology and the way organisations may collect information about individuals.
- CCTV video recordings - captured and stored for the purposes of holding data relating to employee monitoring, staff security and crime prevention

---

Our General Practice

Our General Practice ensures personal data on our patients and staff is processed fairly and lawfully.

Purpose and legal basis for processing your personal data

Our health care professionals who provide you with care maintain records about your health and any treatment or care you have received previously (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.

We want to make sure that you clearly understand why we process your personal information fairly and lawfully for these main reasons:

- the data subject (i.e. the patient) has given consent to the processing of his or her personal data for one or more specific purposes (e.g. to support the delivery of your care);
- processing is necessary for compliance with a legal obligation to which the controller is subject (every General Practice has to record its care provided);
- processing is necessary in order to protect the vital interests of the data subject or of another natural person (i.e. the health and wellbeing of a patient);
- 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 (NHS England and its Clinical Commissioning Groups are tasked by the UK Government to obtain a picture of the health and needs of the local population).

How we prevent illness with 'Risk Stratification' – A term we use in the NHS to describe how information can help improve your health and wellbeing.

'Risk stratification' data tools are increasingly being used by the NHS on computer systems to help determine a person's risk of suffering from a particular illness or condition - preventing an unplanned or (re)admission and identifying a need for preventive intervention.

This means that automated-decision making and profiling of patients is performed by the NHS based upon the information about you that is collected from a number of sources including this General Practice and NHS Trusts. A risk score is arrived at through an analysis of your de-identified information (so you cannot be personally identified at this stage) using computer software, and is only provided back to your General Practice as data controller in an identifiable form.

Risk stratification enables your GP to focus on preventing your 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 by contacting our General Practice - contact details are included at the end of this Practice Privacy Notice.

Medicines Management – Reviewing your prescriptions

Your GP Practice supports a medicines management review service of medications prescribed to its patients. This service involves a review of prescribed medications to ensure patients receive the most appropriate, up to date and cost-effective treatments. This service is provided by qualified and registered healthcare professionals from within the GP practice, our NHS Primary Care Network, NHS North Yorkshire Clinical Commissioning Group or by external partners approved by the GP practice. Patient identifiable information does not leave the practice system but is accessed to ensure only appropriate clinical recommendations or decisions are made for each patient. Each patient can opt out of (or back into) the practice using their data for anything other than specified purposes or where there is a lawful requirement to do so.

The Yorkshire & Humber Shared Record

Yorkshire & Humber Care Record

The Yorkshire & Humber Care Record is a shared system that allows healthcare staff within the Humber, Coast and Vale Health and Social Care community to appropriately access the most up-to-date and correct information about patients to deliver the best possible care. The Yorkshire & Humber Care Record Guarantee is our commitment that we will use records about you in ways that respect your rights and promote your health and wellbeing. If you would like any further information, or would like to discuss this further, please contact our Practice Manager or Caldicott Guardian.

Electronic Palliative Care Co-ordination System (EPaCCS) in Humber, Coast and Vale

EPaCCS enables the recording and sharing of a patient's care preferences and key details about their care at the end of their life. As the patient's preferences are stored electronically, they can easily be shared 24/7 between all of the clinicians and carers involved in the patient's care, whenever and wherever they need it.

An EPaCCS record can be created, updated and shared by any member of a patient's health and care team, subject to locally-determined pathway and user administration settings. EPaCCS is a summary record, intended to provide an easily accessible view of the information that carers need in an end of life situation.

Our practice, along with other health and social care organisations, deliver end of life care to patients. We are all data controllers with a shared purpose of using EPaCCS.

To find out more about EPaCCS and how it supports end of life care in Humber, Coast and Vale, please visit the following website: https://humbercoastandvale.org.uk/how/digital-futures/#EPaCCS.

Personal information that relates to you will be received from a number of areas. Some of the information about your medical history, such as medications and conditions, will come from your GP record. Information about your preferences for how and where you receive care at the end of your life will be provided by you when you share this information with different health and care professionals that deliver your care.

We only collect the personal information necessary about you in order to help us deliver the right service or meet legal obligations.

The information we will share about you is to make sure your preferences and wishes are respected. These include:

- Demographic details (name, contact details, NHS number and gender)
- Any medications you use
- Diagnoses and problems
- CPR decision
- Preferred placed of care
- Preferred place of death.

Your information will be used to make sure that health and care providers involved directly in delivering your care know how to deliver the best EoLC. It's important that your preferences are well known and shared with everyone that cares for you.

CCTV Cameras – Employee Monitoring, Staff Security & Crime Prevention

Our General Practice may make CCTV video recordings that are captured and stored for the purposes of holding data relating to employee monitoring, staff security and to also identify individuals engaged in criminal activity on our premises. This footage is of sufficient quality to identify individuals and will be made available to the police should they legally request to view it. Our CCTV recordings are stored securely and encrypted wherever possible. Individuals have the right to request a copy of any CCTV footage in which they are in focus and/or clearly identifiable. If the request is valid and permissible we can supply the individual with that footage within 30 days of the validation.

GPES Data for Pandemic Planning and Research (COVID-19)

Scarborough Medical Group is supporting vital coronavirus (COVID-19) planning and research by sharing your data with NHS Digital.

The health and social care system is facing significant pressures due to the coronavirus (COVID-19) outbreak. Health and care information is essential to deliver care to individuals, to support health, social care and other public services and to protect public health. Information will also be vital in researching, monitoring, tracking

and managing the coronavirus outbreak. In the current emergency it has become even more important to share health and care information across relevant organisations. This practice is supporting vital coronavirus planning and research by sharing your data with NHS Digital, the national safe haven for health and social care data in England.

Our legal basis for sharing data with NHS Digital

NHS Digital has been legally directed to collect and analyse patient data from all GP practices in England to support the coronavirus response for the duration of the outbreak. NHS Digital will become the controller under the General Data Protection Regulation 2016 (GDPR) of the personal data collected and analysed jointly with the Secretary of State for Health and Social Care, who has directed NHS Digital to collect and analyse this data under the COVID-19 Public Health Directions 2020 (COVID-19 Direction).

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.

Under GDPR our legal basis for sharing this personal data with NHS Digital is Article 6(1)(c) - legal obligation. Our legal basis for sharing personal data relating to health, is Article 9(2)(g) – substantial public interest, for the purposes of NHS Digital exercising its statutory functions under the COVID-19 Direction.

The type of personal data we are sharing with NHS Digital

The data being shared with NHS Digital will include information about patients who are currently registered with a GP practice or who have a date of death on or after 1 November 2019 whose record contains coded information relevant to coronavirus planning and research. The data contains NHS Number, postcode, address, surname, forename, sex, ethnicity, date of birth and date of death for those patients. It will also include coded health data which is held in your GP record such as details of:

- diagnoses and findings
- medications and other prescribed items
- investigations, tests and results
- treatments and outcomes
- vaccinations and immunisations

How NHS Digital will use and share your data

NHS Digital will analyse the data they collect and securely and lawfully share data with other appropriate organisations, including health and care organisations, bodies engaged in disease surveillance and research organisations for coronavirus response purposes only. These purposes include protecting public health, planning and providing health, social care and public services, identifying coronavirus trends and risks to public health, monitoring and managing the outbreak and carrying out of vital coronavirus research and clinical trials. The British Medical Association, the Royal College of General Practitioners and the National Data Guardian are all supportive of this initiative.

NHS Digital has various legal powers to share data for purposes relating to the coronavirus response. It is also required to share data in certain circumstances set out in the COVID-19 Direction and to share confidential patient information to support the response under a legal notice issued to it by the Secretary of State under the Health Service (Control of Patient Information) Regulations 2002 (COPI Regulations).

Legal notices under the COPI Regulations have also been issued to other health and social care organisations requiring those organisations to process and share confidential patient information to respond to the coronavirus outbreak. Any information used or shared during the outbreak under these legal notices or the COPI Regulations will be limited to the period of the outbreak unless there is another legal basis for organisations to continue to use the information.

Data which is shared by NHS Digital will be subject to robust rules relating to privacy, security and confidentiality and only the minimum amount of data necessary to achieve the coronavirus purpose will be shared. Organisations using your data will also need to have a clear legal basis to do so and will enter into a data sharing agreement with NHS Digital. Information about the data that NHS Digital shares, including who with and for what purpose will be published in the NHS Digital data release register.

For more information about how NHS Digital will use your data please see the NHS Digital Transparency Notice for GP Data for Pandemic Planning and Research (COVID-19).

How the NHS and care services use your information

Scarborough Medical Group is one of many organisations working in the health and care system to improve care for patients and the public.

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

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

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

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

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

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

To find out more or to register your choice to opt out, please visit www.nhs.uk/your-nhs-data-matters. On this web page you will:

- See what is meant by confidential patient information

- Find examples of when confidential patient information is used for individual care and examples of when it is used for purposes beyond individual care
- Find out more about the benefits of sharing data
- Understand more about who uses the data
- Find out how your data is protected
- Be able to access the system to view, set or change your opt-out setting
- Find the contact telephone number if you want to know any more or to set/change your opt-out by phone
- See the situations where the opt-out will not apply

You can also find out more about how patient information is used at:
https://www.hra.nhs.uk/information-about-patients/ (which covers health and care research); and
https://understandingpatientdata.org.uk/what-you-need-know (which covers how and why patient information is used, the safeguards and how decisions are made)

You can change your mind about your choice at any time.

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

Health and care organisations have until 2020 to put systems and processes in place so they can be compliant with the national data opt-out and apply your choice to any confidential patient information they use or share for purposes beyond your individual care. Our organisation 'is / is not currently' compliant with the national data opt-out policy.

Your rights over your personal data

To read more about the health and care information NHS Digital collects, its legal basis for collecting this information and what choices and rights you have in relation to the processing by NHS Digital of your personal data, see:

the NHS Digital GPES Data for Pandemic Planning and Research (COVID-19) Transparency Notice

the NHS Digital Coronavirus (COVID-19) Response Transparency Notice

the NHS Digital General Transparency Notice

how NHS Digital looks after your health and care information

Your Medical Records

Medical records can be defined as a "chronological written account of a patient's examination and treatment that includes the patient's medical history and complaints, the physician's physical findings, the results of diagnostic tests and procedures, medications and therapeutic procedures."

Can I ask for my personal NHS Summary Care Medical Records to be deleted?

There is no absolute 'right to be forgotten' on General Practice computer systems. Patients can ask for their personal data to be erased when there is no compelling reason for its continued processing. Requests by our patients will be assessed on their own merits. We have very good reasons for lawfully processing much of the personal information we hold for the purposes of providing continued patient and community care. In summary patients need to understand how medical records benefit both their own health needs and those of the broader population. Some of the purposes why your personal medical records need to be processed are:

- To ensure you receive the best possible care, your records are used to facilitate the ongoing treatment and emergency care you receive from the NHS – for example in a medical emergency it could be critical for a clinician to know if you suffer allergic reactions to certain medicines.
- Information held about you may be used to help protect the health of the public and to help us manage the NHS.
- NHS England and its Clinical Commissioning Groups are tasked by the UK Government to obtain a picture of the health and needs of the local population.
- Information may be used within our General Practice for clinical audit to monitor the quality of the service we provide.
- 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 – our surgery will always gain your consent before releasing the information for this purpose.

Can I obtain how my Information is processed and used elsewhere?

You have the right to control how medical information about you is processed, used, shared, disseminated or sold, for purposes other than your direct medical care - so called secondary uses (or purposes).

Secondary uses include projects involved in risk stratification, "population health management", national clinical audits, research, healthcare planning, commissioning of healthcare services by CCGs, commercial and even political uses.

You can control your personal confidential information by expressing an objection, or '*opt-out'* to our surgery, we will then add a special read code to your GP record.

One such opt-out is known as a ***Type 1 opt-out*** (sometimes referred to as a **XaZ89 or 9Nu0** opt-out).

Type 1 opt-out

A Type 1 opt-out when present in your GP record should prevent identifiable information about you being extracted from your GP record, and uploaded to **any** other organisation, for purposes other than your direct care.

If you request a Type 1 opt-out then it will prohibit extraction and uploading for all of the following secondary uses:

- Risk stratification schemes
- National clinical audits (such as the National Diabetes Audit)
- The Clinical Practice Research Datalink (CPRD)
- Extraction of de-identified information about you concerning any eMed3 (i.e. fit notes)
- Statement of Fitness to Work reports (i.e. sick notes), uploaded to NHS Digital, and subsequently passed by NHS Digital to the Department of Work and Pensions

- All extractions and uploading of identifiable information about you to NHS Digital, for any secondary purpose (so-called GPES extractions)

Electronic Patient Records (EPR) System

Our practice uses an EPR (Electronic Patient Record) computer service supplied by an NHS-approved health it systems company who are located in England - for storing and processing your medical records digitally. Your personal data is referred to as a Summary Care Record.

This system has been developed to help us treat our patients more effectively and to give healthcare staff quicker and easier access to up-to-date information about your treatment. All practice staff who are directly involved with your care will have some level of access to this system, which will be updated at each point of a patient's care. Your personal EPR is referred to as a **Summary Care Record** - an example of a database that processes your data for primary medical uses only, that is for the provision of direct medical care by healthcare professionals. Your records will include important information about your health, including medical history, medications, current prescriptions, allergies, laboratory test results, radiology images, immunisation status and more. It will also include the required personal information we need for our records, including name, date of birth, address, contact phone number and next of kin contact details.

Who can see my NHS Summary Care Record?

Here at the practice we have tight controls in place to ensure that only those directly involved in your care will be allowed access to your Electronic Patient Record and they will only have access to the relevant parts of your Electronic Patient Record that they need in order to do their job. Therefore, anyone who has access to your records:

- Must be directly involved in your care and treatment at the practice
- Will have been assigned a secure access method which uniquely identifies them
- Will only see the information they need to do their job
- Will have their details recorded for every action that is taken on the system

How long do you keep medical records for?

NHS England requires that GP records should be retained until 10 years after the patient's death or after the patient has permanently left the country, unless they remain in the European Union. Unless the GP is notified otherwise the record must be retained for 100 years.

Children and Young People Records: NHS England requires that all types of records for children and young people should be retained until the patient is 25 (or 26 if they are 17 when treatment ends) or eight years after their death, if sooner. If a child's illness or death could be relevant to an adult condition or have genetic implications for their family, records may be kept for longer.

Maternity Records (Inc. Obstetric and Midwifery Records): NHS England requires that maternity records must be retained for 25 years after the birth of the last child.

Mental Health Records: NHS England requires that records of people who have been treated for a mental disorder should be retained for 20 years after the date of last contact between the patient and any healthcare professional employed by the mental health provider, or 8 years after the death of the patient if sooner.

Electronic Repeat Dispensing (eRD)

If you or someone you care for uses the same medicines regularly, you may be able to benefit from electronic repeat prescriptions. This means you won't have to re-order or collect your repeat prescriptions from the practice every time you need more medicine.

If your GP thinks that you could use electronic repeat prescriptions for your regular medicine, they will ask you for your permission to share information about your treatment with your pharmacist. This will help your pharmacist to give your GP feedback about your treatment and provide you with useful advice.

Your GP will then authorise a number of electronic repeat prescriptions to be sent electronically to your nominated pharmacy. This will be based on your circumstances and individual need. These electronic prescriptions will then be supplied to you by your pharmacy at regular intervals.

Important Notice:

Temporary change to need for patient consent to enable increased use of eRD

Patients who receive repeat electronic prescriptions and are considered clinically suitable may receive their medication by way of eRD.

It has always been the case that patients need to individually consent to receiving their medication in this way. Now, using the powers granted by the National Health Service (Amendments Relating to the Provision of Primary Care Services During a Pandemic etc.) Regulations 2020, it has been agreed with the Secretary of State that in certain circumstances (defined below) this requirement can be temporarily suspended.

Practices in England may transfer any clinically suitable patient onto eRD if they are already receiving, or have agreed to receive, electronic prescriptions.

This means:

• Any patient who has previously had medication dispensed by means of the electronic prescription service (EPS); or

• Any patient who has recorded a nominated pharmacy either via the practice, pharmacy or NHS App; or Classification: Official 2

• Any patient whose practice is live with EPS Phase 4.

Our Privacy Promise

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

Scarborough Medical Group Promise:

- To keep your personal data safe and private.
- To give you ways to manage and review how we process and control your data.
- Not to sell your personal data.
- To handle personal data only in ways that patients would reasonably expect.
- Have a basis in law for collecting and using your data and to not do anything unlawful with it.

- Not use your data in ways that are unfair (e.g. in ways you have not been told about and would not expect; where you have a choice but have not had an opportunity or been told how to exercise it; or where the use has an unjustified adverse effect).
- To be open and transparent about how we intend to use your data and who we will share it with.
- 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 in exceptional circumstances (e.g. life or death situations) or if the law requires it to be passed on.

We also operate in accordance with an information sharing principle following Dame Fiona Caldicott's (The UK Government's appointed National Data Guardian for health and social care) information sharing review; *Information to share or not to share* - "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. They are supported by the policies of their employers, regulators and professional bodies.

How the law protects your confidentiality

We are committed to protecting your privacy and will only use information collected lawfully in accordance with:

- Data Protection Act 2018 (based on the EU's GDPR – General Data Protection Regulations)
- 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
- Gender Recognition Act 2004
- Freedom of Information Act 2000

Our legal obligations to protect your personal data

This General Practice is registered with the UK's Information Commissioners Office (ICO) and complies with the Data Protection Act 1998 and its replacement the Data Protection Act 2018. The law is being updated to reflect a European-wide legal framework that applies from 25 May 2018 onwards and is designed to help improve the protection of personal data of individuals – such as our patients and staff.

This includes protection against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage of your data. It requires that appropriate technical or organisational measures are used – so we have policies, procedures and staff training in place to keep your personal data private.

UK and European law demands that in order for our processing to be fair, the 'data controller' (our General Practice who is in control of processing medical records) has to make certain information available to patients or 'data subjects' by allowing you to make a Subject Access Request - contact details are included at the end of this Practice Privacy Notice should you wish to make a request.

Our duty of confidentiality

Under common law our General Practice has a legal duty of confidentiality to safeguard the confidential health data of our patients. Because we control patient healthcare records on paper and digitally we are classed as a responsible 'public authority' as well as a 'data controller' by the Information Commissioners Office (ICO) – this is because we decide how, why, what, when and for how long personal data of our patients are processed.

Implied Consent

Healthcare providers such as our General Practice generally operate on the basis of implied consent to use patient medical records for the purposes of direct patient care, without breaching confidentiality.

However - we cannot rely on a patient's implied consent to use their confidential personal data for other non-direct patient care related activities and therefore we must justify any processing under another lawful basis, such as explicit patient consent or legal gateway.

Our partner organisations

We may 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
- NHS Commissioning Support Units
- Independent Contractors such as dentists, opticians, pharmacists
- Private Sector Providers
- Voluntary Sector Providers
- Ambulance Trusts
- Clinical Commissioning Groups (CCG's)
- Social Care Services
- Health and Social Care Information Centre (HSCIC)
- Local Authorities
- Education Services
- Fire and Rescue Services
- Police & Judicial Services
- Other 'data processors' which you will be informed of such as TPP SystmOne and EMIS

Note: in some cases you will be asked for explicit consent for personal data sharing when this is required. 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.

Organisations other than those listed above that we currently hold contracts with and share data:

- **MJOG Texting service** - your name and mobile telephone number are shared for the purposes of sending appointment reminder messages, Friends and Family Survey requests and recall requests.
- **AccuRx Texting service** – your name and mobile telephone number are shared for purposes of sending appointment reminder messages, links to specific healthcare advice and recall requests.
- **National Diabetes Audit** – your NHS number, date of birth, postcode and information about your diabetes care is extracted by NHS Digital to help the NHS improve care. You have the right to opt out of

this audit. Further information can be found at https://digital.nhs.uk/data-and-information/clinical-audits-and-registries/national-diabetes-audit

- **GP Connect** – your NHS number. This software enables Out of Hours services to book an appointment with the GP directly into the practice's appointment system.

- **iGPR -** We use a processor, iGPR Technologies Limited ("iGPR"), to assist us with responding to report requests relating to your patient data, such as subject access requests that you submit to us (or that someone acting on your behalf submits to us) and report requests that insurers submit to us under the Access to Medical Records Act 1988 in relation to a life insurance policy that you hold or that you are applying for. iGPR manages the reporting process for us by reviewing and responding to requests in accordance with our instructions and all applicable laws, including UK data protection laws. The instructions we issue to iGPR include general instructions on responding to requests and specific instructions on issues that will require further consultation with the GP responsible for your care.

Subject Access Requests and Data Portability

You have a right under the Data Protection Act (as amended) to request access to view or to obtain copies of what information our surgery holds about you and to have it amended should it be inaccurate.

In some circumstances you may also request the erasure of your personal data that we hold. In order to request this, you need to do the following:

- Your request must be made in writing to our Data Controller (details below).
- For information from the hospital you should write directly to them.
- Normally there is no charge to have a printed copy of the information we hold about you. However, we may refuse to comply with a request for erasure if it is 'manifestly unfounded or excessive', taking into account whether the request is repetitive in nature. If we consider that your request fits this description, we will justify our decision in writing to you by:
    - requesting a "reasonable fee" in advance to cover our excess administration costs to deal with a very complex request; or
    - refuse to deal with your request - providing a clear justification.
- We are required to respond to you within one month, unless it is a complex request - which we will inform you of. Then we are required to respond to you within two further months.
- 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.

Requesting a copy or transfer of your data – Referred to as 'Data Portability'

You have the right to data portability. This allows patients to obtain and reuse their personal data they have provided to us for their own purposes across different services – for example, if you migrate to a foreign country you may wish us to transfer or transmit your EPR (Electronic Patient Record) directly to your new healthcare provider who is not part of the NHS - so they can import your medical records into their own IT system.

Patients need to complete our Subject Access Request (SAR) form to request a digital or paper copy of their data or to request an electronic transfer of the data to another data controller.

1. In the first instance we prefer to signpost patients to **NHS Patient Online** – a website where you can view your personal GP record (which includes coded information about allergies, immunisations, diagnoses, medication and test results).

2. In other instances - we can securely email you details of your Summary Care Record via **Encrypted NHS Mail**. This will require your access to a personal email account and a web-browser – so you can setup a free NHS online account to unlock and view your safeguarded medical records that are encrypted by NHS Digital.
3. Alternatively, we can provide your personal medical records as **digital files** – as either text (.txt format) or spreadsheet (.csv format) documents via a secure web transfer service.

In all of the above instances we will need you to verify your identity to ensure that your personal medical records are only released to you - or an appointed person you have authorised us to send your confidential data to.

Website Cookies

Website cookies are small computer files that get sent down to your PC, tablet or mobile phone by websites when you visit them. They stay on your device and get sent back to the website they came from, when you go there again. Cookies store information about your visits to that website, such as your choices and other details. Some of this data does not contain personal details about you or your business, but it is still protected by this Patient Privacy notice. By using our website you agree that we can place these types of cookies on your device, however you can block these cookies using your web browser settings. Our General Practice may use these different types of cookies on our website…

Session Cookies (Temporary Only)

Session cookies last only for the duration of your visit and are deleted when you close your browser. These facilitate various tasks such as allowing a website to identify that a user of a particular device is navigating from page to page, supporting website security or basic functionality. Many of the cookies we use are session cookies. For example, they help us to ensure the security of your session, and can also keep you signed in to our website while you move between pages or service your online account. Our session cookies used for security are designed to be very difficult to use except by us when you have an active session. They contain no personal information that can be used to identify an individual.

Persistent Cookies (Last forever unless cleared by you)

Persistent cookies last after you have closed your browser, and allow a website to remember your actions and preferences. Sometimes persistent cookies are used by websites to provide targeted content based upon the browsing history of the device. We use persistent cookies in a few ways, for example - to remember you have visited our website before and to prevent us showing you a ‘Cookie Information’ banner being shown every time you revisit the website. We also use persistent cookies to allow us to analyse customer visits to our site. These cookies help us to understand how web visitors arrive at and use our site so we can improve our online service.

First and Third Party Cookies

Whether a cookie is a first or third party cookie depends on which website the cookie comes from. First party cookies are those set by or on behalf of the website visited. All other cookies are third party cookies. We use both first party and third party cookies.

Performance Cookies

These cookies collect information about how visitors use a web site, for instance which pages visitors go to most often, and if they get error messages from web pages. These cookies don't collect information that identifies a

visitor although they may collect the IP address of the device used to access the site. All information these cookies collect is anonymous and is only used to improve how a website works, the user experience and to optimise our content messages.

Functionality Cookies

These cookies allow the website to remember choices you make (such as your name in a form). They may also be used to provide services you have requested such as watching a video. The information these cookies collect is anonymised (i.e. it does not contain your name, address etc.) and they do not track your browsing activity across other websites.

Targeting Cookies

These cookies collect several pieces of information about your browsing habits. If we use them they are usually placed by advertising networks. They remember that you have visited a website and this information is shared with other organisations such as media publishers. These organisations do this in order to provide you with targeted adverts more relevant to you and your interests. This type of advertising is called online behavioural advertising and place an icon in the top right hand corner of an advert. This icon when clicked, will take you through to the website Your Online Choices where there is more help and guidance for you to Opt-out of this type of advertising. You can block these cookies using your browser settings.

General Practice contacts for personal data

Data Protection Officer (DPO)

The DPO for the practice is Liane Cotterill. You can contact them at liane.cotterill@nhs.net or on 01642 745042 if:

I. You have any questions about how your information is being held;
II. You require access to your information or if you wish to make a change to your information;
III. You wish to make a complaint about anything to do with the personal and healthcare information we hold about you;
IV. You have any other query relation to this policy and your rights as a patient.

Data Controller

The practice is legally classified as a Data Controller because of the way we process personal data of patients and staff. Our entire organisation is responsible for keeping your information secure and confidential – however our main representative for handling your personal data related questions or Subject Access Requests (SAR) is our Data Protection Officer (DPO).

Complaints

Should you have any concerns about how your personal information is managed by our General Practice please contact the Practice Manager using the details above. If you are still unhappy following a review by our practice you can then complain directly to the Information Commissioners Office (ICO):

Website: www.ico.org.uk **Email:** casework@ico.org.uk **Tel:** 0303 1231113 (local rate) or 01625 545745

Note: Our Practice has no control over other websites that we may link to. We make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to those websites or the information contained within them.