Privacy Notice & Fair Processing

Update: Covid-19 and the use of your information

To look after your healthcare needs during the current coronavirus pandemic, we may need to share your personal information including health and care records with clinical and non-clinical staff who belong to organisations that are permitted to use your information and need to use it to help deal with the Covid-19 pandemic. This means that we may need to share your personal information for the purposes of treating you or a member of your family, and to allow us and other healthcare organisations to monitor the disease, assess risk, track and manage the spread of the disease. We may also need to use your information and health data to enable digital consultations and diagnoses, although we will always do this with your security in mind. We will only share your personal information when it is necessary to meet your needs or to meet public healthcare needs. It may also take us longer to respond to Subject Access requests whilst we focus our efforts on responding to the outbreak. During this period of emergency, opt-outs will not generally apply to the data used to support the Covid-19 outbreak, due to the public interest in sharing information. This includes National Data Opt-Outs. However, in relation to the Summary Care Record, existing choices will be respected.

Some of our staff may need to work from home during this time and may have access to any necessary personal and/or medical information in order to look after your healthcare needs. All staff are required to follow the necessary security policies of the Practice to ensure that all information is kept safe, secure and confidential.

NHS England and Improvement and NHSX have developed a single, secure store to gather data from across the health and care system to inform the Covid-19 response. This includes data already collected by NHS England, NHS Improvement, Public Health England and NHS Digital. New data will include 999 call data, data about hospital occupancy and A&E capacity data as well as data provided by patients themselves. All the data held in the platform is subject to strict controls that meet the requirements of data protection legislation.

These are temporary measures introduced by the Secretary of State for Health and Social Care under Regulation 3(4) of The Health Service (Control of Patient Information) Regulations 2002 to enable organisations to respond to and deal with the Covid-19 pandemic. Unless a further extension is required, these measures will expire on 31 March 2021.

If you are experiencing Covid-19 symptoms we may need to collect specific health data about you. Where we need to do so, we will not collect more information than we require and we will ensure that any information collected is treated with the appropriate safeguards.

Please note *that the data protection and electronic communication laws do not stop us from sending public health messages to you, either by phone, text or email, as these messages are not direct marketing.*

GP Connect

GP Connect is a programme run by NHS Digital that makes information held in GP practice IT systems available across health and social care. This allows other health organisations such as the new NHS 111 service, Covid-19 Clinical Assessment Service (CCAS), to see a 'read only' view of your record at this practice, and based on this information they will be able to directly book you a patient assessment at the Practice. The CCAS service has been set up to assess suspected COVID-19 patients needing further assessment from primary care, but not requiring hospital treatment.

Online Consultations

This Practice has reduced the number of face to face consultations available and during this period of emergency we may offer you a consultation via telephone or via video-conferencing using AccuRx. By accepting the invitation and entering the consultation you are agreeing to this. As part of the clinical assessment during these electronic consultations, patients may be asked to show intimate areas either during a video consultation, or by sending an image to the GP. Your personal/confidential patient information will be safeguarded in the same way it would be with any other consultation. E-Consult and AccuRx are secure, encrypted and approved for use by NHS England. It is also fully auditable and is held on hardware devices that are also encrypted and password protected.

The Practice does not record video consultations or store images received, unless your GP would ordinarily have taken an image during a face to face appointment. If your GP deems it necessary to take an image of your symptoms during a video consultation for your medical record, or to share with a specialist for a second opinion, they will ask your permission, as they would usually do during a face to face consultation. In this instance the image will be included in your record and shared securely if necessary. Images are retained as part of the medical record in line with standard retention periods for GP records. If your GP would normally have described your symptoms in writing for your medical record during the course of a face to face consultation, they will continue to do so from the video and/or image and then securely dispose of any video and/or images received.

Patients should not feel pressured into providing medical consent for the use of video consultations and/or images in place of face to face consultations and can request a face to face appointment instead. Refusal to take part in a video consultation or provide an image will not affect the care that you receive. Your GP may also request that a face to face appointment is made if it is felt that circumstances are not suitable for a video consultation, or provision of an image.

Update: General Practice Extraction Service (GPES) Data

This practice is supporting coronavirus (COVID-19) planning and research by sharing your data with NHS Digital, the national safe haven for health and social care data in England. This information will be vital in researching, monitoring, tracking and managing the coronavirus outbreak. NHS Digital has been legally directed by the Secretary of State for Health and Social Care to collect and

analyse patient data from all GP Practices in England under the COVID-19 Public Health Directions 2020 to support the coronavirus response for the duration of the outbreak. NHS Digital will become the controller under the GDPR 2016 of the personal data collected and analysed jointly with the Secretary of State for Health and Social Care. 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 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. 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. The application of the National Data Opt-Out to information shared by NHS Digital will be considered on a case by case basis and may or may not apply depending on the specific purposes for which the data is to be used. This is because during this period of emergency, the National Data Opt-Out will not generally apply where data is used to support the coronavirus outbreak, due to the public interest and legal requirements to share information.

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), the NHS Digital Coronavirus (COVID-19) Response Transparency Notice, the NHS Digital General Transparency Notice, and how NHS Digital looks after your health and care information.

Overview of information held and shared

Stour surgery aims to ensure the highest standard of medical care for our patients. To do this we keep records about you, your health and the care we have provided or plan to provide to you.

Being transparent and providing accessible information to patients about how we will use your personal information is a key element of the Data Protection Act 2018 and the EU General Data Protection Regulations (GDPR).

This Privacy Notice explains and describes how this GP Practice uses and manages the information it holds about its patients, service users and staff. This includes how the information may be shared with other NHS organisations and with non-NHS organisations, and how the confidentiality of information is maintained.

This privacy notice does not provide exhaustive details of all aspects of the collections and use personal information by Stour Surgery. However we are happy to provide any additional information or explanation needed. As your registered GP practice, we are the data controller for any personal data that we hold about you.

What type of information do we hold about our patients?

We collect and process the following information about our patients:

- identity details – name, date of birth, NHS Number;
- contact details – address, telephone, email address;
- 'Next of Kin' details – the contact details of a close relative or friend;
- details of any carer you may have, or anyone you care for;
- details of any appointments with the GPs and nursing staff;
- reports from secondary care of any A&E visits, inpatient stays or clinic appointments;
- results of any scans, X-rays and pathology tests requested;
- details of any diagnosis and treatments given;
- details of any longstanding health concerns and conditions;
- details about your health, treatment and care and other relevant information from health professionals, care providers or relatives who care for you;
- information about any allergies;
- information about any DNAR decisions and any living wills that we know of;
- correspondence from other Health and Social Care providers that provide you with services.

We work with a number of Health and Social care organisations and independent treatment centres in order to provide you with the best possible care and options for treatment. Your information may therefore be shared securely to provide continuity of care.

Sharing patient information

We know that good communication with other healthcare professionals involved in your care is beneficial to you, and so we work closely with many organisations in order to provide you with the best possible care. This means that if another healthcare professional or service is involved in your care, it might be appropriate to share information with them in order for you to receive the required care.

Your information will be shared between those involved in providing health care services and treatments to you. This includes doctors, nurses and allied health professionals, but may also include administrative staff who deal with booking appointments or typing clinic letters.

Access to information is strictly controlled and restricted to those who need it in order to do their jobs. All of our staff receive annual mandatory training on confidentiality and data security and also have strict contractual clauses within their employment contracts which oblige them to respect data protection and confidentiality.

Who we share with

The Practice shares and receives patient information from a range of organisations or individuals for a variety of lawful purposes, including:

- disclosure to hospitals and other NHS staff for the purposes of providing direct care and treatment to the patient, including administration;
- disclosure to social workers or to other non-NHS staff involved in providing health and social care;
- disclosure to specialist employees or organisations for the purposes of clinical auditing;
- disclosure to those with parental responsibility for patients, including guardians;
- disclosure to carers without parental responsibility;
- disclosure to medical researchers for research purposes (subject to explicit consent, unless the data is anonymous);
- disclosure to NHS managers and the Department of Health for the purpose of planning, commissioning, managing and auditing healthcare services;
- disclosure to bodies with statutory investigative powers e.g. the Care Quality Commission, the GMC, the Audit Commission and Health Services Ombudsman;
- disclosure to national registries e.g. the UK Association of Cancer Registries;
- commissioning support units;
- NHS Digital;
- NHS 111;
- COVID Clinical Assessment Service (CCAS)
- MJog for the purposes of providing appointment reminders by text messaging;
- AccuRx for the purposes of e-consultation, video calling or text messaging you to provide or request health information related to your direct care and treatment;
- Attend Anywhere for providing a secure video call service for video consultations for the purposes of providing direct care and treatment;
- education services;
- fire and rescue services – emergency;

- ambulance trusts;
- voluntary sector providers;
- independent contractors such as dentists, opticians, pharmacists;
- disclosure to solicitors, insurance companies, the police, the Courts (including a Coroners Court) and to tribunals and enquiries.

Confidential patient identifiable information is only shared with other organisations where there is a legal basis to do so, such as:

- when there is a Court Order or a statutory duty to share patient data;
- where there is a statutory power to share patient data;
- when the patient has given his/her explicit consent to the sharing;
- when the patient has implicitly consented for the purpose of direct care;
- when the sharing of patient data without consent has been authorised by the Health Research Authority's Confidentiality Advisory Group (HRA CAG) under s.251 of the NHs Act 2006.

Patient identifiable information is only shared on a need to know basis, where there is a direct purpose to do so, limited to what is necessary for that purpose. Patient information may be shared, for the purposes of providing direct patient care, with other NHS provider organisations such as NHS Acute Trusts (hospitals), NHS Community Health, other NHS General Practitioners (GPs), NHS Ambulance services in order to maintain patient safety; this data will always be identifiable. For the purposes of commissioning and managing healthcare, patient information may also be shared with other types of NHS organisations such as the local Clinical Commissioning Group (CCG), and NHS England. In such cases, the shared data is made anonymous or pseudonymised, wherever possible, by removing all patient identifiable details, unless the law requires the patient's identity to be included.

For the benefit of the patient, the Practice may also share information with non-NHS organisations which are also providing healthcare. These non-NHS organisations may include, but are not restricted to: social services, education services, local authorities, the police, voluntary sector providers, and private sector providers.

Patients are not legally or contractually obliged to share information with their healthcare provider however, your care will be affected if your clinicians do not have the relevant information necessary in order to diagnose and treat you. If you have set sharing and opt-out preferences these will be respected where there is no lawful obligation to share the information.

Purposes of processing, retention and your rights

Purposes of processing

Our Practice processes patient data for the following primary purposes:

- providing direct healthcare;
- providing other healthcare providers with information regarding your healthcare;
- supporting social care with safeguarding vulnerable patients.

We keep records in order to:

- have accurate and up to date information available to the right care and treatment options;
- have information available to clinicians that you may see or be referred to at another NHS organisation or organisation providing NHS services.

Summary Care Record (SCR)

There is a national NHS healthcare records database provided and facilitated by NHS England, which holds your Summary Care Record (SCR). Your SCR is an electronic record which contains information about the medicines you take, allergies you suffer from and any bad reactions to medicines you have had.

Storing information in one place makes it easier for healthcare staff to treat you in an emergency, or when your GP Practice is closed. This information could make a difference to how a doctor decides to care for you, for example which medicines they choose to prescribe for you.

Only healthcare staff involved in your care will access your Summary Care Record. When you are registered with a GP Practice in England your Summary Care Record is created automatically. It is not compulsory to have a Summary Care Record. If you choose to opt-out, you need to inform the Practice.

For further information about SCR, visit the NHS Digital website.

Enhanced Summary Care Record (eSCR)

With your consent, additional information can be added to your Summary Care Record in order to provide more tailored care to you.

Other information that you can choose to include could be:

- information about you long term health conditions - such as asthma, diabetes, heart problems or rare medical conditions;
- information about your relevant medical history – clinical procedures that you have had, why you need a particular medicine, the care you are currently receiving and clinical advice to support your future care;
- information about your health care preferences – you may have your own care preferences which will make caring for you more in line with your needs, such as special dietary requirements;
- information about your personal preferences – you may have personal preferences, such as religious beliefs or legal decisions that you would like to be known;
- information about your immunisations – details of previous vaccinations, such as tetanus and routine childhood jabs;
- specific sensitive information – such as any fertility treatments, sexually transmitted infections, pregnancy terminations or gender reassignment will not be included, unless you specifically ask for any of these items to be included.

Additional information is only included in your SCR when you request it, for further information about including additional information on your SCR, visit the NHS Digital website.

GP clinical system - electronic patient records

Our Practice uses an electronic patient record to securely process and share information between NHS staff. This means that healthcare professional who is caring for you can see your medical history, including any allergies and current medications, to provide you with safe care.

Our Practice uses SystmOne as our Electronic Patient Record. You can find out more about SystmOne on the TPP Website here: https://www.tpp-uk.com/products/systmone

Enhanced data sharing model (EDSM) in SystmOne

We are able to share clinical information about your health and care requirements held on your SystmOne electronic patient record with other health organisations including other GP practices, child health services, community health services, hospitals, out of hours, continuing healthcare team at the CCG and other similar organisations. This means that the healthcare professional looking after you has the most relevant information to enable them to provide you with the most appropriate care. We automatically set up the sharing facility in our electronic patient record system to allow your information to be shared out to other health organisations.

Local trusted organisations that we work with on a regular basis are able to access your record immediately once they have asked your permission. If you say "no" they will not be able to see any information. An audit log is maintained, showing who accessed your record and when it was accessed. You are entitled to request a copy of this log.

If you see a healthcare professional outside your local geographic area (who also uses SystmOne), and you agree that they can have access to your medical records, you will be asked to provide additional security details in the form of a verification code which is sent to you either as a text, email or via your SystmOnline account. It is therefore important that we always have your up-to-date contact details.

If you do not wish us to share your information in this way, please let us know at Reception and we will ensure that your information is not shared.

Primary care networks

Primary Care Networks (PCNs) are groups of GP Practices working closely together with their local partners (e.g. other primary and community care staff, mental health, social care, pharmacy, hospital and voluntary services for the benefit of patients and the local community. Our Practice is part of Christchurch PCN, alongside Highcliffe Medical Centre, Christchurch Medical Practice and Farmhouse Surgery.

Working as part of a network rather than a stand-alone business means that the GP Practices in our PCN can share expertise and resources which means that we can offer a wide range of services to

suit the needs of our local community to give you the best possible care. You may be seen by clinicians from anywhere in our PCN, at any of our Practices. In order that they can give you the best possible care, they will have access to your health data. Only healthcare staff involved in your care will have access to your record.

Dorset care record (DCR)

Health and social care organisations in Dorset may hold different sets of records about you, and not every organisation uses SystmOne. The Dorset Care Record is a confidential computer record that joins up all these different records to create one complete and up to-date record. Sharing appropriate information electronically to a single place, offers direct access for authorised health and social care professionals to provide as full a picture as possible of your history, needs, support and service contacts.

If you do not wish your information to be shared in this way, you will need to opt-out of the Dorset Care Record. You can do this by contacting the Privacy Officer on the DCR website. The Dorset Care Record have their own Privacy Notice, available on the website.

Dorset integrated care system (ICS)

Dorset's integrated care system, known locally as 'Our Dorset' is a partnership of local organisations working together to improve services to meet the needs of local people and deliver better outcomes. 'Our Dorset' aims to see every person in Dorset stay healthy for longer and feel more confident and supported in managing their own health. The partnership includes:

- Dorset Clinical Commissioning Group;
- Foundation Trusts: Dorset County Hospital, Poole Hospital, The Royal Bournemouth and Christchurch Hospitals, Dorset Healthcare University and South Western Ambulance Service;
- Bournemouth Borough Council, Borough of Poole Council and Dorset County Council;
- Public Health Dorset.

'Our Dorset' have a 'Dorset Intelligence and Insight' (DiiS) Business Intelligence platform which uses pseudonymised data to reveal important insights into local and community health care, in order to inform the future of health care for communities. Information is pseudonymised so that when a new service is introduced to help with a particular long term condition in a particular community, the Practice can ask for any of their own patients to be re-identified from the data in order to invite you to use the new service. If you are signed up to the National Data Opt-Out, your information will not be used in the DiiS.

Diabetic eye screening

The Dorset Diabetic Eye Screening Programme is provided by Health Intelligence Ltd, commissioned by NHS England South (Wessex) as part of the National Diabetic Eye Screening Programme. We share information with Health Intelligence in order to provide diabetic retinopathy screen for our diabetic patients.

You can find out more about the Diabetic Eye Screening on their website.

Our practice website

Our website does not use cookies to track your activity online but the "remember these details" feature on our on-line prescription form uses first party cookies on your computer to store your information. This information is only used to remember your details and is never passed to any third party. Cookies must be enabled in your browser for this feature to work. Using this feature means you agree to the use of cookies.

Individual funding request

An 'Individual Funding Request' is a request made on behalf of a patient, by a clinician, for funding of specialised healthcare which falls outside the range of services and treatments that NHS Dorset Clinical Commissioning Group (CCG) has agreed to commission for the local population.

An Individual Funding Request is taken under consideration when a case can be set out by a patient's clinician that there are exceptional clinical circumstances which make the patient's case different from other patients with the same condition who are at the same stage of their disease, or when the request is for a treatment that is regarded as new or experimental, and where there are no other similar patients who would benefit from this treatment.

A detailed response, including the criteria considered in arriving at the decision, will be provided to the patient's clinician.

Invoice validation

Invoice validation is an important process. It involves using your NHS number to check which CCG is responsible for paying for your treatment. We can also use your NHS number to check whether your care has been funded through specialist commissioning, which NHS England will pay for. The process makes sure that the organisations providing your care are paid correctly.

Other ways in which patient information may be used:

Incident management

If you are involved in an incident, for example you slip and fall whilst in the Practice, your information may be included in the incident report and used as part of the investigation process.

Recorded telephone calls

We record all incoming and outgoing telephone calls to and from the Practice for the following purposes:

- to help with staff training (in this instance a transcript of the call is created which contains no patient identifiable or sensitive information);
- to enable us to obtain the necessary facts in the event of a complaint;
- for patient telephone consultations (in this instance a transcript of the call is created and entered into the individual patient health record);
- for medico-legal purposes; and
- for quality assurance to allow us to audit and improve our service to you.

Recordings of telephone calls will only be accessed where necessary by the Practice management team. Recordings are stored in accordance with the Records Management Code of Practice for Health and Social Care 2016 Retention Schedule, after which they are deleted.

Complaints and queries

If you raise a complaint or query with the Practice, the team will hold information about you within their secure database in order to ensure that your complaint or query is answered appropriately by the relevant person or department. Details of complaints or queries will not be stored within your medical records.

Secondary uses

We may also process data for the following secondary uses:

- **Clinical Research:** sometimes your information may be requested to be used for research purposes – the practice will always gain your consent before using information for this purpose;
- **Clinical Audit:** information may be used for audit to monitor the quality of the service provided. Some of this information may be held centrally and used for statistical purposes. Where this is done we make sure that individual patient records cannot be identified, e.g. the National Diabetes Audit. Audits will have approval from the Clinical Advisory Group, under s.251 of the NHS Act 2006 and data submissions will be signed off by our Caldicott Guardian;
- **Improving Services:** the CCG will sometimes extract pseudonymised medical information about you to help identify areas for improvement in the services provided to you.
- **Risk Stratification:** data tools are increasingly being used in the NHS to help determine a person's risk of suffering a particular 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. A risk score is then arrived at through an analysis of your de-identified information using software managed by NHS approved third parties and is only 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;
- **National Archiving:** records made by an NHS organisation are Public Records in accordance with Schedule 1 of the Public Records Act 1958. The Public Records Act 1958 requires organisations to select core records for permanent preservation at the relevant Place of Deposit (PoD) appointed by the Secretary of State for Culture, Media and Sport. PoDs are usually public archive services provided by the relevant local authority. The selection and transfer must take place at or before records are 20 years old and is a separate process from appraisal for retention to support current service provision. Potential transfers of digital records should be discussed with the PoD in advance to ensure that technical issues can be resolved. Records no longer required for current service provision may be temporarily retained pending transfer to a PoD and records containing sensitive personal data should not normally be transferred early.

These secondary uses help the NHS to:

- prepare and analyse statistics on NHS performance;
- audit NHS services, locally and nationally;
- monitor how we spend public money;
- plan and manage health services for the population of Dorset;
- conduct health research and development of treatments.

Our Practice values the concept of data minimisation and will use anonymised or pseudonymised information as much as possible. We rely on Articles 6(1)(e) and Articles 9(2)(h) for lawfully processing identifiable data. Where you have opted-out of the use of identifiable data for secondary purposes, your data will not be used unless it is anonymised or unless there is a legal obligation for us to process it.

National data opt-out

The national data opt-out was introduced on 25 May 2018, enabling patients to opt out from the use of their data for purposes beyond their individual care, such as 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.

Patients can view or change their national data opt-out choice at any time by using the online service at www.nhs.uk/your-nhs-data-matters, or by calling 0300 3035678. Further information is available 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).

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.

Data controller and processors

The Practice is the Data Controller of the data which we gather, hold and create about you.

The Practice engages with data processors who may process your data. All Data Processors are held to strict contractual obligations, which specify the limitations, any access arrangements, storage and retention of data on our behalf as well as strict confidentiality and information

handling clauses. All data processors are also held to high information security standards and asked to provide evidence of how they met Data Protection legislation. These processors may be software suppliers or specialist and support services.

Transfers to third countries or international organisations

The Practice does not routinely transfer data outside of the European Economic Area and will assess any adhoc transfers against adequacy (GDPR Article 45) and appropriateness of safeguards and data protection (GDPR Article 46) of the country of transfer.

Retention periods

The Practice works to the Records Management Code of Practice for Health and Social Care 2016 Retention Schedule. https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

Data subject rights

The law gives you certain rights to your personal healthcare information that we hold:

1. Right of access to your information

You have the right to request a copy of the personal information that we hold about you; this is known as a Subject Access Request. We have one month to reply to you and give you the information that you require. This can be extended by two further months if the request is complex or we have received a number of requests from you. Subject Access Requests can be made by you the patient, by a legal representative; a solicitor acting on your behalf, a carer, parent, guardian or appointment representative, with appropriate consent. A personal representative also has the right of access to deceased records. If you would like a copy of the information we hold about you, please let us know. For more information please see our Subject Access Request policy.

We will provide this information free of charge however, we may in some limited and exceptional circumstances have to make an administrative charge for any extra copies if the information requested is excessive, complex or repetitive.

We can restrict disclosure of your information if your doctor feels that granting access would disclose information likely to cause serious harm to your physical or mental health or that of another individual, and where you do not already know the information. Or where granting access would disclose information relating to or provided by a third party who could be identified from the information, and who has not provided consent for it to be released.

2. Right to restrict or object to the use of your information

We cannot share your information with anyone else for a purpose that is not directly related to your health without your consent. Patients have the right to restrict the processing of your personal information for secondary purposes through NHS Digital's National Data Opt-Out. More information is available here.

The right to restrict processing of healthcare data can only be exercised in the following circumstances:

- the accuracy of the data is contested;
- the processing is unlawful.

3. Right to have incorrect information corrected

If you feel that information held about you is incorrect, you have the right to ask for it to be corrected. This applies to matters of fact, not opinion. Incorrect contact information such as your address will be corrected immediately. If the information is of a clinical nature, this will need to be reviewed and investigated by the Practice, which will result in one of the following outcomes:

- the Practice considers the information to be correct at the time of recording and will not amend the data. A statement from you may be placed within the record to demonstrate that you disagree with the information held. You have the right to appeal to the Information Commissioner;
- the Practice agrees that the information is incorrect, however it is not legal to modify or remove information within the record as it represents 'historical information' which may have influenced subsequent events of decisions made. In these circumstances, a note will be made in the record which advises the reader of the inaccuracy and of the correct facts. The Practice will agree the content of the note with you.

4. Right to data portability

This right only applies where the original processing is based on the data subject's consent or fulfilment of a contract that they are party to, and if the processing is automated. However, in the spirit of the Regulations, you have the right to request that your personal and/or healthcare information is transferred, in and electronic or other form, to another organisation.

5. Right to appropriate decision making

The right to appropriate decision making applies to automated processing, including profiling, which produces legal outcomes, or that significantly affects you. The Practice has not identified any automated processing which is solely automated and without human involvement in the outcome of the processing.

6. Right to erasure

This is sometimes known as 'the right to be forgotten', but it is not an absolute right. You cannot ask for this right of erasure in relation to records which the Practice is legally bound to retain. The Practice has an obligation, not only to retain information for a specified time period, but also not to retain information for longer than is necessary and will dispose of information securely.

Please see above section on retention.

7. Right to lodge a complaint

If you are dissatisfied with the handling of your personal information, you have the right to make a complaint. In the first instance, formal complaints should be addressed to the Practice Manager.

You also have the right to make a complaint to the Information Commissioner's Office – the independent regulator of data protection:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Or using their online submission: https://ico.org.uk/global/contact-us/

The law explained

Data Protection Principles

There are six core principles to data protection legislation:

1. Personal data must be processed lawfully, fairly and transparently (lawfulness, fairness and transparency).
2. Personal data must be collected for specific, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes (purpose limitation).
3. Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
4. Personal data must be accurate and up to date (accuracy).
5. Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed (storage limitation).
6. Personal data is processed in a manner that ensures appropriate Security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

Lawful basis

The Practice processes personal data for **primary purposes** under the following legal basis:

- **General Data Protection Regulation 2016/679 Article 6(1)(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"

For the processing of personal data for secondary purposes the Practice may rely on one of the following legal bases depending on the circumstances:

- **General Data Protection Regulation 2016/679 Article 6(1)(c):**

"processing is necessary for compliance with a legal obligation to which the controller is subject"

There are some National Audits and patient registers which require the Practice to process your information under Article 6(1)(c) in accordance with UK legislations such as the National Health Service Act 2006 and Health and Social Care (Safety and Quality) Act 2015.

There are also obligations within the Crime and Disorder Act 1998, Terrorism Act, Children's Act(s) 1989 and 2004, Mental Health Act 1983 and 2007 to share information with the Police or Social Services.

The Practice processes special categories of data (health data) for primary purposes under the following legal bases:

- **General Data Protection Regulation 2016/679 Article 9(2)(h):**

"Processing is necessary for the purposes of preventative 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 and social care systems and services on the basis of Union or Member State law or pursuant to contact with a health professional and subject to the conditions and safeguards referred to in paragraph 3"

Paragraph 3: *"Personal data referred to in paragraph 1 [special categories of data] may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of a professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies."*

- **General Data Protection Regulation 2016/679 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 in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and interests of the data subject"

The Practice processes special categories of data for secondary purposes under the following legal bases:

- **General Data Protection Regulation 2016/679 Article 9(2)(j):**

"Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subjects"

- **General Data Protection Regulation 2016/679 Article 9(2)(i):**

"Processing is necessary for reasons of public interest in the areas of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality

and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy."

Where data has been anonymised it is not considered to be personal data and the General Data Protection Regulation 2016/679 and Data Protection Act 2018 will not apply. The Practice will use anonymous data for audit and population health management.

Occasionally, the Practice may rely on consent as a legal basis:

- **General Data Protection Regulation 2016/679 Article 6(1)(a):**

"the data subject has given consent to the processing of his or her personal data for one or more specific circumstances"

Where you are asked for your consent to take part in Research, Clinical Trials or Audits, your care will not be affected if you decline to take part. Research and Audit are vital for the NHS to evaluate and improve Healthcare for everyone.

- **General Data Protection Regulation 2016/679 Article 9(2)(a):**

"the data subject has given explicit consent to the processing of those personal data for one of more specified purposes"

However, these circumstances will be few and the Practice will not rely on consent where there is another lawful basis that we should use.

- **General Data Protection Regulation 2016/679 Recital 43** specifies that for consent to be freely given it

"should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation."

Our Practice upholds transparency and fairness through the use of this privacy notice. We uphold data minimisation techniques like pseudonymisation and anonymisation where possible to protect data and ensure that the purpose of processing is relevant and adequate.

The Practice holds data security in the highest importance; our systems have role-based access and clinical systems are auditable to ensure transparency in the use of systems by staff. Devices are encrypted and all our staff undertake annual mandatory data security training.