Wareham Surgery Privacy Notice

Tier One – Overview of information held and shared

This Privacy Notice explains and describes how this GP Practice uses and manages the information it holds about its patients and service users. 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.

Our contact details

Practice Name	Wareham Surgery
Address	Streche Road, Wareham, Dorset, BH20 4PG
Phone number	01929 553444
Email	Wareham.surgery@nhs.net
Data Protection Officers	Helen Williams and Lynda Bennett NHS Dorset ICB
Data Protection Registration Number	Z4960240

What type of personal information do we hold about our patients?

We currently collect and process the following information about our patients:

- identity details – name, gender, sexual orientation, 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 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 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 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 screening programmes and 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);
- Department for Work and Pensions to improve the monitoring of public health and commissioning and quality of health services through the provision of anonymised data on patients who have been issued with a fit note under the Fit for Work scheme;
- MJog for the purposes of providing appointment reminders, service updates and communications by text messaging;
- AccuRx for the purposes of e-consultation, video calling (using a data processor, Whereby) 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;
- iGPR for the purposes of responding to requests for medical reports and subject access requests;
- Immedicare for the purposes of enabling video calling for assessment and clinical decision making in nursing and residential care homes;
- Abtrace for the purposes of proactive monitoring and recall;
- approved health app providers to allow you to enter your own health data into the apps for clinical observation and monitoring;
- 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 NHS Dorset, 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 health, care and emergency/front line services. 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 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.

Tier Two – 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 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 England website.

Enhanced Summary Care Record (eSCR)

With your consent, additional information can be added to your Summary Care Record to provide more tailored care to you. Other information that you can choose to include could be:

- information about your 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 England website.

Electronic Patient Check-in – Numed Envisage

Wareham Surgery uses the Numed Envisage Patient Check-in system to allow patients to check in electronically when arriving for appointments.

When using the touchscreen, patients are asked to enter limited identifying information, including their date of birth and the first letter of their surname. This information is used to identify their appointment securely through our clinical system, SystmOne, provided by The Phoenix Partnership (TPP).

The system processes the information necessary to identify the patient and record their arrival. Numed provides and supports the check-in system and may have limited access to information when providing authorised technical support.

The information is processed to support the safe and efficient delivery of NHS healthcare services.

The lawful bases for processing under UK GDPR are:

- **Article 6(1)(e):** Processing necessary for the performance of a task carried out in the public interest.
- **Article 9(2)(h):** Processing necessary for the provision and management of health or social care.

Patients who do not wish to use the electronic check-in system, or who require assistance, can continue to check in with our reception team.

Use of AI-Assisted Workflow Processing (Anima)

Wareham Surgery uses secure digital systems, including AI-assisted technology provided by Anima Health, to support the processing of incoming clinical correspondence and administrative workflows.

This technology is used to assist practice staff with tasks such as:

- Summarising clinical documents
- Identifying document types
- Suggesting coding or routing options
- Supporting efficient document management workflows

The system is designed to support administrative efficiency and improve the timely handling of patient information. It does not replace clinical judgement or decision-making.

All information processed remains under the control of Wareham Surgery as the Data Controller. Anima Health acts as a Data Processor on behalf of the practice and is contractually required to comply with UK GDPR, NHS data security standards, and confidentiality requirements.

Any AI-generated suggestions are reviewed by appropriately trained staff before information is added to the clinical record or acted upon.

Only the minimum necessary information is processed, and appropriate technical and organisational security measures are in place to protect patient data.

GP Connect

We use a facility called GP Connect to support your direct care. GP Connect makes patient information available to all appropriate clinicians when and where they need it, to support direct patient care, leading to improvements in both care and outcomes. GP Connect is not used for any purpose other than direct care.

Authorised Clinicians such as GPs, NHS111 Clinicians, Care Home Nurses (if you are in a Care Home), Secondary Care Trusts, Social Care Clinicians are able to access the GP records of the patients they are treating via a secure NHS Digital service called GP connect.

The NHS 111 service (and other services determined locally e.g. other GP Practices in a Primary Care Network) will be able to book appointments for patients at GP Practices and other local services. For additional information about the GP Connect facility, visit the NHS Digital website.

OpenSAFELY

NHS England has been directed by the Government to establish and operate the OpenSAFELY service. This service provides a Trusted Research Environment that supports COVID-19 research and analysis. Each GP practice remains the controller of its own patient data but is required to let researchers run queries on pseudonymised patient data. This means identifiers are removed and replaced with a pseudonym, through OpenSAFELY. Only researchers approved by NHS England are allowed to run these queries and they will not be able to access information that directly or indirectly identifies individuals. More information about OpenSAFELY is available here.

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 the 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, or further details on sharing in SystmOne can be found here.

Enhanced data sharing model (EDSM) in SystmOne

We can 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 NHS Dorset 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 for the purpose of direct patient care.

Local trusted organisations that we work with on a regular basis can 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 Purbeck PCN, alongside Swanage, Corfe Castle, Wool, Bere Regis and Sandford Practices

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.

Social Prescribing

Social prescribing enables GPs, nurses and other primary care professionals to refer patients to a range of local, non-clinical community services to help patients to improve their health, wellbeing and social welfare. This can include advice and information on local services and connecting individuals to social activities, clubs, groups, and like-minded individuals in the community. For example, signposting people who have been diagnosed with dementia to local dementia support groups. The Practice will do this by employing someone to act as a 'link' between the Practice, the patient and the non-clinical services within the community. Current providers in our area include:

- Livewell Dorset
- Help and Care

We will refer you to one of these providers and will send basic information such as name, NHS number, address, date of birth and background to your health and wellbeing needs. The providers are bound by confidentiality in the same way that Practice staff are, and there is a Data Sharing Agreement in place to ensure that personal data is used in a lawful and appropriate way. More information about social prescribing can be found on the NHS England website.

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. This provides direct access for authorised health and social care professionals to obtain 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 Board (ICB)

Dorset's integrated care board, named 'NHS Dorset', undertakes the statutory responsibilities of the previous Clinical Commissioning Group (CCG) and is responsible for healthcare planning to meet the needs of people and communities in Dorset. NHS Dorset will work more closely with other NHS organisations and local authorities in Dorset's integrated care system, known locally as 'Our Dorset' to improve services to meet the needs of local people and deliver better outcomes. The partnership includes:

- Foundation Trusts: Dorset County Hospital NHS Foundation Trust, University Hospitals Dorset NHS Foundation Trust, Dorset Healthcare University NHS Foundation Trust and South Western Ambulance Service NHS Foundation Trust;
- Bournemouth, Christchurch and Poole Council, and Dorset Council;
- Public Health Dorset;
- People and communities within Dorset.

NHS 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, 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.

Should any patient request to opt out of the DiiS, the code to apply is: "Declind consent use pt data in rsk stratifctn unplnnd admiss XabjB (928671000000101"

Diabetic eye screening

The Dorset Diabetic Eye Screening Programme is provided by NEC Care, commissioned by NHS England South (Wessex) as part of the National Diabetic Eye Screening Programme. The programme supports your invitation for eye screening and ongoing care by the screening programme. Your information may be shared with any Hospital Eye Services you are under the care of to support further treatment, and with other healthcare professionals involved in your care. We also share information with Health Intelligence in order to provide diabetic retinopathy screening for our diabetic patients.

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

Diabetes prevention programme

The Healthier You: NHS Diabetes Prevention Programme is provided in Dorset by 'Live Well Taking Control (LWTC)', commissioned by NHS England, as part of the National Diabetes Prevention Programme. This programme identifies those at high risk of Type 2 diabetes and refers them onto a behaviour change programme run by 'Live Well Taking Control'.

You can find out more about the Diabetes Prevention Programme on their website.

ACR project for patients with diabetes (and/or other conditions)

The data is being processed for the purpose of delivery of a programme, sponsored by NHS Digital, to monitor urine for indications of chronic kidney disease (CKD) which is recommended to be undertaken annually for patients at risk of chronic kidney disease e.g., patients living with diabetes. The programme enables patients to test their kidney function from home. We will share your contact details with Healthy.io to enable them to contact you and send you a test kit. This will help identify patients at risk of kidney disease and help us agree any early interventions that can be put in place for the benefit of your care. Healthy.io will only use your data for the purposes of delivering their service to you. If you do not wish to receive a home test kit from Healthy.io we will continue to manage your care within the Practice. Healthy.io are required to hold data we send them in line with retention periods outlined in the Records Management code of Practice for Health and Social Care. Further information about this is available at: https://lp.healthy.io/minuteful_info/.

Third Party Service Providers

We may employ professional services from companies such as Help & Care and Dorset Mind to deliver services on our behalf.

All professional service providers are required to take appropriate security measures to protect your data in line with Practice policies. We do not allow them to use your data for their own purposes. We permit them to process your data only for specified purposes and in accordance with our instructions.

Where your data is shared with third parties, we will seek to share the minimum amount necessary.

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 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 ICB 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 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 for one month, after which they are deleted.

SMS communications

If you have provided us with your mobile telephone number, we may use this to send you SMS messages relating to your healthcare. These may include automatic appointment reminders or cancellations, reminders of clinics, invitations to screening, medication reviews, vaccination appointments, requests to complete surveys or to make you aware of services provided by the surgery that we feel will be to your benefit, or to update you about local and national health promotions. If you do not wish to receive these messages, please let the reception team know.

Email communications

Where you have provided your email addresses for communication purposes, we may contact you when necessary to do so for direct health care purposes or to provide you with service updates that relate to the essential task and function of the Practice. Electronic communication is a more efficient and cost-effective method of communicating with you. The Practice aims to keep communication to a minimum, but if you do not wish to receive these messages, please let the reception team know.

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:** NHS Dorset 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. Through the Dorset Intelligence & Insight Service (DiiS) we are working to improve short term and medium-term health outcomes for local populations through the application of Population Health Management and Analysis. The DiiS, set up and run by NHS staff across Dorset and hosted within Dorset HealthCare, pseudonymise at source and extract the data to analyse the use of services and identify areas for prevention and improvement in overall patient health and well-being outcomes. A small number of specialist analytics staff from NHS Trusts manage this data within the DiiS platform. In addition, the DiiS work with Sollis to provide risk stratification of this data which 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 including social prescribing.
- **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 UK GDPR 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

Whenever you use a health or care service, important information about you is collected in your patient record for that service 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. 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.

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.

Our Practice is compliant with the national data opt-out policy which means that we have systems and processes in place to comply with the national data opt-out so that your choice can be applied to any confidential patient information we 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 are asked to provide evidence of how they meet Data Protection legislation. These processors may be software suppliers or specialist and support services.

Cross Border Transfers between the UK, the EU, other third countries or international organisations

Following the UK's exit from the European Union the UK has now become a third country under the EU GDPR. An adequacy decision for the UK has been approved by the EU Commission under Article 45(3) of the EU GDPR, allowing the free flow of personal data between the EU and the UK to continue. The Practice does not routinely transfer data outside of the European Economic Area and will assess any adhoc transfers against adequacy (UK GDPR Article 45) and appropriateness of safeguards and data protection (UK GDPR Article 46) of the country of transfer.

Retention periods

The Practice works to the NHS Records Management Code of Practice Retention Schedule.

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 contact:

Wareham Surgery Admin
Streche Road
Wareham
Dorset
BH20 4PG

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 an 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 to 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:

Practice Manager
Wareham Surgery
Streche Road
Wareham
Dorset
BH20 4PG

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/

Tier Three – 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

From 1 January 2021, the 'UK GDPR' has replaced the GDPR as the UK's data protection law. The Practice processes personal data for **primary purposes** under the following legal basis:

- **UK General Data Protection Regulation 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:

- **UK General Data Protection Regulation 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:

- **UK General Data Protection Regulation 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."

- **UK General Data Protection Regulation 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:

- **UK General Data Protection Regulation 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"

- **UK General Data Protection Regulation 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 UK General Data Protection Regulation 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:

- **UK General Data Protection Regulation 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.

- **UK General Data Protection Regulation 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.

- **UK General Data Protection Regulation 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.