

## **PRIVACY NOTICE**

**We understand how important it is to keep your personal information safe and secure and we take this very seriously. We have taken steps to make sure your personal information is looked after in the best possible way and we review this regularly.**

**Please read this privacy notice ('Privacy Notice') carefully, as it contains important information about how we use the personal and healthcare information we collect on your behalf.**

### **How we use your personal information**

This privacy notice explains why the practice collects information about patients, members of staff and visitors to the practice, known as Data Subjects and how we use your information. So that we can provide you with the best possible service, a variety of information is collected about you from a range of sources, such as your local NHS hospitals. This information is used to support your healthcare. Under the UK General Data Protection Regulation (UK GDPR) information about your physical and mental health, racial or ethnic origin and religious belief are considered as special category (sometimes known as sensitive) personal information and is subject to strict laws governing its use. This page explains why the Practice collects personal information about you, the ways in which such information may be used, and your rights under the UK General Data Protection Regulation. The Practice is legally responsible for ensuring its processing of personal information is in compliance with the general data protection regulation. The practice becomes what is known as the data controller, which simply means that we are responsible for maintaining the security and confidentiality of the personal information that you provide us with.

### **Security of Information**

Confidentiality affects everyone: Thornbury Medical Centre collect's, stores and uses large amounts of personal and sensitive personal data every day, such as medical records, personnel records and computerised information. This data is used by many people in the course of their work.

We take our duty to protect personal information and confidentiality very seriously and we are committed to comply with all relevant legislation and to take all reasonable measures to ensure the confidentiality and security of personal data for which we are responsible, whether computerised or on paper.

The partners have appointed a Senior Information Risk Owner who is accountable for the management of all information assets and any associated risks and incidents, and a Caldicott Guardian who is responsible for the management of patient information and patient confidentiality.

## **Legal Basis for processing your information**

Under UK GDPR the Practice are mandated to identify a legal basis to process your personal information.

### **Special Category data (Sensitive Data including Health Records)**

- Explicit consent
- Employment, social security and social protection (if authorised by law)
- Vital interests – Life and Death
- Made public by the data subject
- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)
- Public health (with a basis in law)

For personal data

- **Consent:** the individual has given clear consent to process their personal data for a specific purpose.
- **Contract:** the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- **Legal obligation:** the processing is necessary for you to comply with the law (not including contractual obligations).
- **Vital interests:** Life & Death
- **Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

## **Why do we collect information about you**

All clinicians and health and social care professionals caring for you keep records about your health and any treatment and care you receive from the NHS. These records help to ensure that you receive the best possible care. They may be paper or electronic and they may include:

- Basic details about you such as name, address, email address, NHS number, date of birth, next of kin, etc.
- Contact we have had with you such as appointments or clinic visits.
- Notes and reports about your health, treatment and care – A&E visits, in patient spells or clinic appointments.
- Details of diagnosis and treatment given
- Information about any allergies or health conditions.
- Results of x-rays, scans and laboratory tests.
- Relevant information from people who care for you and know you well such as health care professionals and relatives.
- For visitors to the practice basic information such as name and vehicle registration number

It is essential that your details are accurate and up to date. Always check that your personal details are correct when you visit us and please inform us of any changes to your contact details. This minimises the risk of you not receiving important correspondence.

By providing the Practice with their contact details, patients are agreeing to the Practice using those channels to communicate with them about their healthcare, i.e. by letter (postal address), by voice mail or voice message (telephone or mobile number), by text message (mobile number) or by email (email address).

## **How your personal information is used**

In general, your records are used to direct, manage, and deliver the care you receive to ensure that:

- The doctors, nurses and other health or social care professionals involved in your care have accurate and up to date information to assess your health and decide on the most appropriate care for you.
- Health or social care professionals have the information they need to be able to assess and improve the quality and type of care you receive.
- Your concerns can be properly investigated if a complaint is raised.
- Appropriate information is available if you see another clinician or are referred to a specialist or another part of the NHS or social care.
- We may offer you a consultation via telephone or videoconferencing. By accepting the invitation and entering the consultation you are consenting to this. Your personal/confidential patient information will be safeguarded in the same way it would with any other consultation.

## **Risk Stratification**

“Risk stratification involves applying computer searches to your medical records from a number of sources, including NHS trusts and GP practices, to identify those patients who are most at risk of certain medical conditions, such as heart disease, and who will benefit from clinical care to help prevent or better treat their condition. It’s a process for identifying and managing patients who are most likely to need hospital or other healthcare services, so that such patients can receive additional care/support from their GP or care team as early as possible. The aim is to prevent ill health and possible future hospital stays, rather than wait for you to become sick.

Section 251 of the NHS Act 2006 provides a statutory legal basis to process personal health related data for risk stratification purposes.

Please be reassured that any information which identifies you - resulting from a forementioned computer searches - will only be seen by this Practice.

If you do not wish information about you to be included in the risk stratification programme, please let us know. We can add a code to your health care record that will stop your information from being used for this purpose. “

## **The NHS care record guarantee**

The Care Record Guarantee is our commitment that we will use records about you in ways that respect your rights and promote your health and wellbeing. Copies of the full document can be obtained from:

**<https://webarchive.nationalarchives.gov.uk/ukgwa/20130513181549/http://www.nigb.nhs.uk/guarantee>**

## **The Records Management Code of Practice**

This Records Management Code of Practice for Health and Social Care 2020 is a guide for the NHS to use in relation to the practice of managing records. It is relevant to organisations who work within, or under contract to NHS organisations in England. This also includes public health functions in Local Authorities and Adult Social Care where there is joint care provided within the NHS.

The Code is based on current legal requirements and professional best practice.

**<https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/>**

## **How long are records retained**

All records are retained and destroyed in accordance with the NHS Records Management Code of Practice.

The Practice does not keep patient records for longer than necessary and all records are destroyed confidentially once their retention period has been met, and the Practice has made the decision that the records are no longer required.

## **When do we share information about you**

We share information about you with others directly involved in your care; and share more limited information for indirect care purposes, both of which are described below.

Everyone working within the NHS has a legal duty to keep information about you confidential. Similarly, anyone who receives information from us also has a legal duty to keep it confidential.

## **Direct Care Purposes**

- NHS Trusts and hospitals that are involved in your care.
- NHS Digital and other NHS bodies.
- Other General Practitioners (GPs) or Primary Care Networks (which are groups of GP Practices).
- Ambulance Services.
- Integrated Care Board's (ICB)

You may be receiving care from other people as well as the NHS, for example Social Care Services. We may need to share some information about you with them so we can all work together for your benefit if they have a genuine need for it or we have your permission. Therefore, we may also share your information, subject to strict agreement about how it will be used, with:

- Social Care Services.
- Education Services.
- Local Authorities.
- Voluntary and private sector providers working with or for the NHS. Such as Dentists, Pharmacies. Opticians & care homes

## **Indirect Care Purposes:**

We also use information we hold about you to:

- Review the care we provide to ensure it is of the highest standard and quality
- Ensure our services can meet patient needs in the future
- Investigate patient queries, complaints and legal claims
- Ensure the hospital receives payment for the care you receive
- Prepare statistics regarding NHS performance
- Audit NHS accounts and services
- Undertake health research and development (with your consent – you may choose whether or not to be involved)
- Help train and educate healthcare professionals
- Health and social care policy, planning and commissioning purposes
- GP Federations
- Public health purposes, including COVID-19

## **Refusing or withdrawing consent**

- The possible consequences of refusing consent will be fully explained to the patient at the time and could include delays in receiving care.
- In those instances where the legal basis for sharing of confidential personal information relies on the patient's explicit or implied consent, then the patient has the right at any time to refuse their consent to the information sharing, or to withdraw their consent previously given.
- In instances where the legal basis for sharing information relies on a statutory duty/power, such as disclosures of notifiable diseases <https://www.gov.uk/guidance/notifiable-diseases-and-causative-organisms-how-to-report> then the patient cannot refuse or withdraw consent for the disclosure.

Nationally there are strict controls on how your information is used for these purposes. These control whether your information has to be de-identified first and with whom we may share identifiable information. You can find out more about these purposes, which are also known as secondary uses, on the NHS England and NHS Digital's websites:

- [www.england.nhs.uk](http://www.england.nhs.uk)
- [www.digital.nhs.uk](http://www.digital.nhs.uk)

## **National Data Opt Out**

“How the NHS and care services use your information”

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

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

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

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

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

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

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

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

You can also find out more about how patient information is used at:

<https://www.hra.nhs.uk/information-about-patients/> (which covers health and care research); and

<https://understandingpatientdata.org.uk/what-you-need-know> (which covers how and why patient information is used, the safeguards and how decisions are made)

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

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

### **OpenSAFELY COVID-19 Service**

The NHS England OpenSAFELY COVID-19 Service is a secure, transparent, open-source software platform for analysis of electronic health data. The system provides access to de-identified (pseudonymised) personal data to support Approved Users (academics, analysts, and data scientists) to undertake approved projects for COVID-19 research, COVID-19 clinical audit, COVID-19 service evaluation and COVID-19 health surveillance purposes.

The purposes for processing are to identify medical conditions and medications that affect the risk or impact of COVID-19 infection on individuals; this will assist with identifying risk factors associated with poor patient outcomes as well as information to monitor and predict demand on health services.

Further information can be found here:

**[The NHS England OpenSAFELY COVID-19 service - privacy notice - NHS Digital](#)**

## **Other ways we use your information**

### **Call recording**

All Telephone calls are routinely recorded for the following purposes:

- To make sure that staff act in compliance with practice procedures.
- To ensure quality control.
- Training, monitoring and service improvement
- To prevent crime, misuse and to protect staff

## **Data Subject Rights**

### **Under the UK General Data Protection Regulation (UK GDPR)**

- A right to confirmation that their personal data is being processed and access to a copy of that data which in most cases will be Free of Charge and will be available within 1 month (which can be extended to two months in some circumstances)
- Who that data has or will be disclosed to.
- The period of time the data will be stored for
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed.
- Data Portability – data provided electronically in a commonly used format
- The right to be forgotten and erasure of data does not apply to an individual's health record or for public health purposes
- The right to lodge a complaint with a supervising authority

## **Your right to object**

You have the right to restrict how and with whom we share information in your records that identifies you. If you object to us sharing your information we will record this explicitly within your records so that all healthcare professionals and staff involved with your care are aware of your decision. If you choose not to allow us to share your information with other health or social care professionals involved with your care, it may make the provision of treatment or care more difficult or unavailable.

Please discuss any concerns with the clinician treating you so that you are aware of any potential impact. You can also change your mind at any time about a disclosure decision.

## **SMS Text messaging**

When attending the Practice for an appointment or a procedure you may be asked to confirm that the Practice has an accurate contact number and mobile telephone number for you. This can be used to provide appointment details via SMS text messages and automated calls to advise you of appointment times.

## **CCTV**

We employ surveillance cameras (CCTV) on and around our practice in order to:

- protect staff, patients, visitors and Practice property
- apprehend and prosecute offenders, and provide evidence to take criminal or civil court action
- provide a deterrent effect and reduce unlawful activity
- help provide a safer environment for our staff

- monitor operational and safety related incidents
- help to provide improved services, for example by enabling staff to see patients and visitors requiring assistance

You have a right to make a Subject Access Request of surveillance information recorded of yourself and ask for a copy of it. Requests should be directed to the address below and you will need to provide further details as contained in the section 'How you can access your records'. The details you provide must contain sufficient information to identify you and assist us in finding the images on our systems.

We reserve the right to withhold information where permissible by the UK General Data Protection Regulation (GDPR) 2018 and we will only retain surveillance data for a reasonable period or as long as is required by law. In certain circumstances (high profile investigations, serious or criminal incidents) we may need to disclose CCTV data for legal reasons. When this is done there is a requirement for the organisation that has received the images to adhere to the UK GDPR.

### **How you can access your health records**

The UK GDPR gives you a right to access the information we hold about you on our records. Requests must be made in writing to the Practice. The Practice will provide your information to you within one month (this can be extended dependent on the complexity of the request) from receipt of your application.

### **Employee Notice**

When you apply for a position within the Practice you will provide us with relevant information about you including:

- A. Your contact details (such as your name and email address, including place of work and work contact details).
- B. Employment history
- C. Qualifications
- D. Referee Details

During the recruitment and selection processes we will begin to add further information including:

- Copies of qualifications and certificates
- Pre-employment checks, including references, identity documents and right to work check information
- Publicly available information such as social media presence
- Selection information including correspondence, interview notes, results of any selection tests that you may be undertake

Following your appointment, we may add any other information you supply to us or is required as part of your employment such as revalidation information.

## **Information about you from others**

Information may be provided about you from a number of sources during your recruitment and on-going employment with the Practice including:

- Disclosure and Barring Service disclosures, where applicable, which will tell the organisation about any criminal convictions you may have
- Referees providing confidential information about your suitability to the role
- Inter Authority Transfer (IAT) – Information held by your previous NHS employer
- Information from HM Revenue and Customs (HMRC) relating to your pay and employment
- Information about your right to work and visa applications
- Pension Information when transferring within the NHS
- Information from your manager and HR team relating to your performance, sickness absence and other work related matters
- Confirmation of your registration with a professional body

## **When do we share information about you**

The Practice may disclose personal and sensitive information with a variety of recipients including:

- Our employees, agents and contractors where there is a legitimate reason for them receiving the information
- Current, past or potential employers of our staff to provide or obtain references
- Professional and regulatory bodies (e.g. Nursing and Midwifery Council (NMC), Health and Care Professions Council (HCPC), General Medical Council (GMC) in relation to the confirmation of conduct including complaints, job description and information provided as part of the recruitment process.
- Government departments and agencies where we have a statutory obligation to provide information (e.g. HMCR, NHS Digital, Department of Health and the Home Office)
- The Disclosure and Barring Service (DBS) and DBS Update Service where we require a DBS check for certain roles
- Third parties who work with us to provide staff support services (e.g. counselling)
- Crime prevention or detection agencies (e.g. the police, security organisations, department for works and pensions and local authorities)
- Internal and external auditors
- Debt collection and tracing agencies
- Courts and tribunals
- Trade union and staff associations
- Survey organisations for example for the annual staff survey

Any disclosures of personal data are always made on case-by-case basis, using the minimum personal data necessary for the specific purpose and circumstances and with the appropriate security controls in place. Information is only shared with those agencies and bodies who have a "need to know" or where you have consented to the disclosure of your personal data to such persons.

## **Legal Basis for processing your data**

The Practice will only ever process your personal information where it is able to do so by law and using one of a number of legal basis available under the Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR).

The legal bases we use are as follows:

### **Special Category data** (Sensitive Data including Health Records)

- Explicit consent
- Employment, social security and social protection (if authorised by law)
- Vital interests – Life and Death
- Made public by the data subject
- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)
- Public health (with a basis in law)

For personal data

- Consent: the individual has given clear consent to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
- Vital interests: Life & Death
- Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

### **Your Individual rights as an employee**

You have certain rights with respect to the data held about you by the Practice.

These are:

- To be informed why, where and how we use your information
- To ask for access to your information
- To ask for your information to be corrected if it is inaccurate or incomplete
- To ask for your information to be deleted or removed where there is no need for us to continue processing it
- To ask us to restrict the use of your information
- To ask us to copy or transfer your information from one IT system to another in a safe and secure way, without impacting the quality of the information
- To object to how your information is used
- To challenge any decisions made without human intervention (automated decision making)

### **How we use the personal data about you**

The Practice uses staff data for all purposes associated with the administration of the employer/employee relationship and to meet our legal obligations. The purposes for which we may use staff data (including sensitive personal information) include:

- Process your recruitment application and correspond with you in relation to Practice vacancies
- Maintaining staff records
- Recruitment and selection
- Managing Human Resource employment matters (e.g. promotion, training and development, conduct, attendance, appraisals, management progress, grievances, misconduct investigations, disciplinary actions and complaints)

- Administering finance (e.g. salary, pension and staff benefits)
- Complying with visa requirements
- Providing facilities such as IT/system access, library services and car parking
- Monitoring equal opportunities
- Preventing and detecting crime, such as using CCTV and using photo's on ID badges
- Providing communication about the Practice, news and events
- Maintaining contact with past employees
- Provision of wellbeing and support services
- Compliance with legal obligations such as making external/statutory returns to NHS England, sharing information with HMRC
- Carrying out research, surveys and statistical analysis (including using third party data processors to carry out the national staff survey)
- Carrying out audits

The Practice processes sensitive personal data for a number of administrative purposes:

- Equal opportunities monitoring
- Managing Human Resources processes such as administering sick pay and sick leave, managing absence, administrating Maternity Leave and associated pay schemes
- Managing a safe environment and ensuring fitness to work
- Managing obligations under Equal Opportunities Legislation
- Provision of Occupational Health and Wellbeing service to individuals
- Payment of trade union membership fees

### **How long are records retained**

All records are retained and destroyed in accordance with the NHS Records Management Code of Practice.

The Practice does not keep patient records for longer than necessary and all records are destroyed confidentially once their retention period has been met, and the Practice has made the decision that the records are no longer required.

We carefully consider any personal information that we store about you, and we will not keep your information for longer than is necessary for the purposes as set out in this Privacy Notice.

### **Freedom of Information**

The Freedom of information Act 2000 provides any person with the right to obtain certain information held by the Practice, subject to a number of exemptions. If you would like to request some information from us, please contact us.

Please note: if your request is for information we hold about you (for example, your health record), please instead see above, under "How You Can Access Your Records".

We may amend this privacy notice at any time so please review it frequently. The date at the top of this page will be amended each time this notice is updated

## **Data Controller**

**The Data Controller responsible for keeping your information confidential is:**

Thornbury Medical Centre

## **Data Protection Officer (DPO)**

The appointed DPO is Daljeet Sharry-Khan [Daljeet.Sharry-Khan@bradford.nhs.uk](mailto:Daljeet.Sharry-Khan@bradford.nhs.uk)

Scorex House (East)

1 Bolton Road

Bradford

BD1 4AS

## **Raising a concern**

Patients who have a concern about any aspect of their care or treatment at the Practice or about the way their records have been managed, should contact the Practice Manager.

If you have any concerns about how we handle your information you have a right to complain to the Information Commissioners Office about it.

UK GDPR requires organisations to lodge a notification with the Information Commissioner to describe the purposes for which they process personal information. These details are publicly available from:

Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

SK9 5AF

Telephone: **0303 123 1113**

Website: [www.ico.org.uk](http://www.ico.org.uk)