University Hospitals Bristol
NHS Foundation Trust

Your rights and how we look after your information

University Hospitals Bristol NHS Trust ("the Trust") is the controller of personal data for the purposes of the Data Protection Act 2018 and the General Data Protection Regulation. The Trust may be contacted at Information Governance, Trust Headquarters, Marlborough Street, Bristol, BS1 3NU. The Trust may also act as a processor of personal data on behalf of partner organisations.

The Trust takes your confidentiality and privacy rights very seriously and we are committed to taking all reasonable measures to ensure the confidentiality and security of personal data for which we are responsible, whether computerised or on paper. This notice explains in detail how we collect, process, transfer and store your personal information and forms part of our accountability and transparency to you under the General Data Protection Regulation (GDPR) 2018.

At Board level, we 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.

If you have any concerns as to how your personal data is processed you can contact the Trust's Data Protection Officer at the above address, by email to InformationGovernance@UHBristol.nhs.uk or by phone at 0117 342 3701.

You can read the Trust's Privacy Notice online here.

Alternatively you can view the information via the sections below:

- Patients
- Trust Membership
- Working for us
- Surveillance Cameras
- Your rights and Subject Access Requests
- Cookies
- Feedback and web forms

We also have a leaflet explaining what we do with your personal information.

Information that may also be of interest:

- Trust Information Governance Policy (pdf)
- Patient Information Principles, Guidelines and Procedures (pdf)
- Our policies and procedures
- Sharing information for Connecting Care
- How to access your medical records

Patients

If you want a basic overview of how we handle patient information please read our leaflet "What we do with your personal information". Full details are set out below.

What Information do we collect from you?

Health and social care professionals working with you – such as doctors, nurses, support workers, psychologists, occupational therapists, social workers and other staff involved in your care – keep records about your health and any care and treatment you receive. This may include:

- Basic details such as name, address, date of birth, phone number, and email address - where you have provided it to enable us to communicate with you by email
- Your next of kin and their contact details
- Notes and reports about your physical or mental health and any treatment, care or support you need and receive
- Results of x-rays, scans, laboratory tests and diagnosis
- Relevant information from other professionals, relatives or those who care for you or know you well
- Any contacts you have with us such as home visits or outpatient appointments
- Information on medicines, side effects and allergies
- If you stay in one of our hospitals, information about your menu choices and meals provided
- Patient experience feedback and treatment outcome information you provide

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 as soon as possible.

Most of your records are electronic and are held on a computer system and secure IT network. New models of service delivery are being implemented, with closer working with GPs and other healthcare and social care providers. To make this possible, the use of other electronic patient record systems to share your information will be implemented. You will be given the opportunity to say no and to object to this sharing. Sharing your information via secure electronic methods, means that necessary information relating to you which is relevant to the care that you need, is shared more quickly and accurately. If you opt out of your information being shared via this method, then this information will still be shared via the slower more traditional routes such as letters, phone calls and emails. See also Connecting Care below.

Why do we collect this information about you?

Your information is used to guide and record the care you receive and is vital in helping us to:

- have all the information necessary for assessing your needs and for making decisions with you about your care
- have details of our contact with you, such as referrals and appointments and can see the services you have received
- assess the quality of care we give you
- ensure that appropriate information is available if you see another doctor, or are referred to a specialist or another part of the NHS, Social Care or another health provider.
- properly investigate if you and your family have a concern or a complaint about your healthcare

Professionals involved in your care will also have accurate and up-to-date information and this accurate information about you is also available if you:

- Move to another area
- Need to use another service
- See a different healthcare professional

What is your legal basis for processing my personal information?

When you consen to treatment we do not rely on that same consent to use your information as a 'legal basis for processing'. We rely on specific provisions under Article 6 and 9 of the General Data Protection Regulation, such as '…a task carried out in the public interest or in the exercise of official authority vested in the controller.'

In particular the Trust has a legal duty under the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 to maintain securely an accurate, complete and contemporaneous record in respect of each service user, including a record of the care and treatment provided to the service user and of decisions taken in relation to the care and treatment provided. Because of this there are limitations on your rights to object to the keeping of records or to ask for them to be deleted. For more information see the section on "Your Rights".

This means we can use your personal information to provide you with your care without seeking your consent.

Other legal duties may require us to use your information for processing a complaint, for assessing, monitoring and improving the quality and safety of the services we

provide, to seek feedback on the quality of services, or for the general management of the NHS.

The NHS is supported by a complex network of statutory duties and powers. We have provided here an overview of the main provisions applying to the Trust. If you require specific information about the particular duty or power supporting any activity please contact the Data Protection Officer:
InformationGovernance@UHBristol.nhs.uk

What else do we use your information for

In addition to using your information for managing your care it may be used for some additional purposes including:

- Planning managing and improving NHS Services. To help us monitor our performance, evaluate and develop the services we provide, it is necessary to review and share minimal information, for example with the NHS Clinical Commissioning Groups. The information we share would be anonymous so you cannot be identified and all access to and use of this information is strictly controlled.
- Clinical audits and other quality improvement projects/activities. We try continually to raise the standard of care we provide. To do this we need to review the clinical work we do, this is typically done using a process known as Clinical Audit. Access to your patient records for this purpose is monitored and only anonymous information is used in any reports that are shared internally with in our Trust.
- Approving payments where you have an individually commissioned care plan
- Recovering costs if you are an out of area patient and some other NHS organisation is responsible for the cost of your care
- Contribute to service development (the Trust may contact patients to raise awareness of the Trust's designated charities, but will not share personal data with them)
- Prepare statistics on NHS performance;
- Internal and External audit of Trust accounts
- Helping to train health professionals. The information you give us is vital in helping us to educate the health workers of the future. However, you always have the right to choose whether not to have students present during a consultation.
- Health research and development - see also the section on use of data for research purposes.

Wherever possible these activities will use anonymised information and in all cases will use only the minimum personal data required. The Trust adopts the principles in the Information Commissioner's Anonymisation Code of Practice which you can find here.

Where we do use information for these purposes we will only do so if there is a proper legal basis to do so – for example an approval under s251 of the National Health Service Act 2006 allows us to use personal data to validate payments for out of area treatments.

In some cases you have the right to opt-out of the use of your information for purposes other than your direct care. See the section on the National Data Opt-Out below.

How long do we keep your records?

There is no single retention period which applies to all medical records. The Trust aims to comply with the Records Management Code of Practice for Health and Social Care 2016.

In general medical records are retained for eight years from data of discharge or end of care but some may be kept longer than that e.g. if there has been a serious incident. For a child the record will be kept until the 25th or 26th birthday depending on age when discharged / last seen.

Exceptions where records may be kept longer – up to 30 years or eight years after death include:

- Cancer / oncology records
- Long term illnesses
- Human Fertilization and Embryology – up to 50 years
- Mental Health issues (20 years)
- Obstetric maternity and neo-natal – 25 years

For full details please see the NHS Retention Schedule

Who might we share your information with?

Your health records are confidential and every member of staff within the NHS has a legal duty to keep your information confidential and secure, ensuring that confidential data about you is used only in the course of their duties and for lawful purposes.

Health and Social Care Professionals - Your information will be shared with the team who are caring for you and are providing treatment to you.

We will share information with the following main partner organisations:

- Other NHS Trusts and hospitals that are involved in your care;
- General Practitioners (GPs); and
- Ambulance Services

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. Therefore, we may also share your information, subject to strict agreement about how it will be used, with:

- Social Care Services;
- Community Pharmacies
- Education Services;
- Local Authorities; and
- Voluntary and private sector providers working with the NHS

We do this in order to provide the most appropriate treatment and support for you, and your carers, or when the welfare of other people is involved. Where practical we will discuss such sharing with you so that there are no surprises but if necessary for your care we will imply your consent for such sharing from your consent to treatment.

You have the right to object to information sharing at any time. Please discuss this with your relevant health care professional as this could have implications in how you receive further care, including delays in receiving care or it may make the provision of treatment and care most difficult or impossible. Objections to sharing will be noted explicitly within your records in order that all healthcare professionals and staff treating you are aware of your decision. You can also change your mind at any time about this sharing.

However, a person's right to confidentiality is not absolute and there may be other circumstances when we must share information from your patient record with other agencies. These are rare circumstances and we are not required to have your consent for these purposes.

Examples of this are:

- If there is a concern that you are putting yourself or another person at risk of serious harm
- If there is concern that you are putting a child at risk of harm
- If we have been instructed to do so by a Court
- If the information is essential for the investigation of a serious crime
- If you are subject to the Mental Health Act (1983), there are circumstances in which your 'nearest relative' must receive information even if you object or we

may need to make a decision in your best interests in accordance with our Mental Capacity policy
- If your information falls within a category that needs to be notified for public health or other legal reasons, such as certain infectious diseases

We would never share your information for marketing or insurance purposes without your explicit and specific consent.

NHS Patient Survey Programme (NPSP) is part of the government's commitment to ensure patient feedback is used to inform the improvement and development of NHS services. We have a legal duty under Regulation 17 of the Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 to assess, monitor and improve the quality and safety of the services provided (including the quality of the experience of service users in receiving those services). We may share your contact information with an NHS approved contractor as a data processor to be used for the purpose of the NPSP.

NHS Digital, on behalf of NHS England assess the effectiveness of the care provided by publicly-funded services - we have to share information from your patient record such as referrals, assessments, diagnoses, activities (e.g. taking a blood pressure test) and in some cases, your answers to questionnaires on a regular basis to meet our NHS contract obligations and our legal duty under s259 Health and Social Care Act 2012. For further information about how NHS Digital looks after your data follow this link.

Clinical Commissioning Groups Information may be shared with a Clinical Commissioning Group where it is necessary for them to comply with their legal duties. For example they have particular duties relating to the discharge of patients under the Care Act 2014 and for the provision of continuing care under s3 NHS Act 2006 including in some cases the authorisation of individual funding. Please also see the Bristol, North Somerset and South Gloucestershire Clinical Commissioning Group Privacy Notice.

NHS England

Where your doctor wants to prescribe certain specialised drugs, approval may be needed from NHS England. In these cases we need to confirm that you meet the required clinical criteria defined by either NICE or NHS England policy. These aim to ensure that treatments are offered to those patients most likely to benefit clinically from them. In order to do this, your doctor will complete a form with your information through a website provided by Blueteq. If you are eligible for the treatment your doctor has prescribed, NHS England will immediately approve this application so you can begin your treatment without delay. Once you have received your treatment, your hospital will ask NHS England for payment for your treatment and NHS England

will go through a process to authorise the payment. To allow NHS England to ensure that it pays for treatments for patients who meet the necessary clinical criteria, your personal details will be processed by NHS Digital teams; NHS Digital is the national safe haven set up under the Health and Social Care Act 2012 - Safe Havens have been set up in the NHS to ensure that confidential patient data can be transmitted and stored securely. NHS Digital will de-identify the data so NHS England can match the clinical approval and payment without being able to link any information to a specific individual. Data which identifies you is only used for your direct care purposes. All data required by NHS England for commissioning purposes is de-identified by NHS Digital in line with the Information Commissioners Code of Practice on Anonymisation. Please also see the NHS England Privacy Notice.

South West Child Health Information Service (CHIS)

For the purposes of providing medical services to, and the safeguarding of, children the Trust shares Maternity Department Data and Newborn Hearing Screening Data with the South West CHIS. This is a Public Health Service commissioned by NHS England to maintain active and accurate child health records for the local population including children who move in and out of the area; manage queries about the health status of individual children and populations; and check who has not yet had their interventions and ensure that no interventions are duplicated or unintentionally missed.

Information is hosted by Health Intelligence Limited who act as Processors for the Trust and other participating health service providers. Information may be made available through the service to NHS Providers/NHS Business Partners under an NHS Contract to deliver Child Health Services including Health Visitor teams, Looked After Children co-ordinators, School Nursing Teams, Acute (including Maternity Departments/Units), Newborn Bloodspot Laboratory, Newborn Hearing Screening Providers, Newborn Infant & Physical Examination (NIPE) providers, Vision Screening Providers, and Mental Health and Community Health service providers who are engaged in delivering services to children.

All parties participating in the CHIS have signed specific Data Sharing Agreements to control their access to this patient data. For further information please see the CHIS section of the Health Intelligence Limited Privacy Notice.

Connecting Care: Connecting Care is a digital care record system for sharing information in Bristol, North Somerset and South Gloucestershire. It allows instant, secure access to a summary of your health and social care records for the professionals involved in your care to help them manage your care better, allowing up-to-date information to be shared quickly and safely.

Connecting Care takes some of the information held in the Trust's medical records together with information from GP practices, other hospitals deprtments, community services, mental health trusts, out of hours services and local authorities across Bristol, North Somerset and South Gloucestershire. This information combines into a single, shared digital record all about you.

The main types of data which may be shared are;

Person Details and Demographics; Other Addresses Held; Immediate Family Members; Legal Relationships; Key Case Worker (s); Last Known GP Practice; Disabilities; Allergies; Events; Medications; Procedures; Examinations; Investigations; Procedures; Referrals Details; Social / Family History; Next of Kin; Alerts, Risks And Warnings; Admissions; Previous Appointments Details; Future Appointment Details; Assessment; Care Plan Interventions Details; Care Plan Problems Details; Care Plans Details; Carer Details; Diagnosis Details; Diagnostic Tests; radiology information; Discharges; DOLs (Deprivation of Liberty); Early Interventions; Risk Management plans; Safeguarding; End of Life Care Plan

Only those directly involved with your care and providing health services across Bristol, South Gloucestershire and North Somerset who are authorised to use the system can see this information. All authorised users of Connecting Care are required to select a legitimate reason for access to a record, otherwise they are unable to access that record. Usually this will be because, being involved in your treatment they require access in order to provide you with safe and effective treatment based on the best available and most up to date information.

The legal basis for holding information within Connecting Care is the same as for the Trust holding your records initially and also as part of the legal duties on the Trust and its partners to improve the services provided to patients.

As the information is confidential to the original provider you do have the right to object to such sharing. However this may have an impact on your care. If you do object the information will be removed from general view but may still be available for some specific purposes such as protecting someone from harm where a legal duty may override your objection. For further information please see What if I don't want my information shared?

We would also refer you to the Transparency Notice of the Connecting Care website.

BUPA / Private Patients:

The Trust has arrangements with health insurance providers including BUPA for the provision of private treatment. In such cases we will share information with the insurer as required by our contract with them for the following purposes:

- To provide clinical quality information
- To notify them of any serious incidents
- To pre-authorise treatment
- To invoice them for services
- To assist them when they are investigating a complaint

You can view BUPA's notice here. You should refer to your insurers own Privacy Notice.

As required by the Competition & Markets Authority Private Healthcare Market Investigation Order 2014 we may share non-identifiable information about you and your treatment with the Private Healthcare Information Network (PHIN). For further details see the PHIN Privacy Notice.

Personal Health Record

The NHS is committed to introducing processes to help patients to see their personal health records online. The aim is that patients should be able to:

- see information that healthcare staff want to share with them
- find out about appointments and treatment
- have more control over their health problems
- bring together information from different NHS organisations they have contact with

The Trust is rolling out a Personal Health Record (PHR) for this purpose using systems provided by System C Healthcare Limited who act as a data processor for the Trust.

Information held within the PHR may include:

- Questions, queries, or feedback you leave, including your email address and mobile number if you provide it to us.
- Details that allow you to access NHS services (you will always be told when this information is being collected, and it will only be used for the purpose you provide it for).
- Personal Confidential Data which you may provide including health diaries, blood pressure, blood sugar, and weight and which will be used for your direct care with your consent or may be used in an anonymised form for research purposes but only with your consent.

Use of a PHR will help us to understand your needs and provide you with a better service as well as providing you with direct access as set out above.

You are not required to have a PHR and accordingly the above information is used with your explicit consent. You can always withdraw that consent by contacting us in which case your PHR can be discontinued.

The PHR will also progressively allow you to have direct access to a range of information including:

- Your details: a view of your personal details held by the Trust including your GP details.
- Your admissions – Any inpatient admissions that you have had to University Hospitals Bristol.
- Any emergency department attendances you have had at University Hospitals Bristol.
- Your Appointments – Your outpatient appointments booked through the University patient administration system
- Questions, queries or feedback you leave, including your email address and mobile number if you provide it to us.
- Direct access to parts of your records including test results (and also information fromcommunity and social care providers)

This information is effectively a snapshot of information held elsewhere by the provider. It is not processed under your consent to have a PHR but for the reasons set out in the main part of this notice or the privacy notice of the provider. If you discontinue your PHR you will lose access but the records will be retained. See also section on your rights.

Teen and Young Adults IAM

The Teen and Young Adults IAM is a web based service which aims to support teenage and young adult patients with cancer. Completing an IAM assessment helps users, the Trust and its partners to understand the patient's needs so we can work together to provide the right support.

Information you provide is given by explicit consent and will only be used at your request and with that consent.

Please also see the TYA IAM Privacy Policy.

Hospital Passport

The Trust uses a Hospital Passport to support the care of adults with learning disabilities and autism when going to hospital. This records your contact details, all essential information we need to know about you, important information about your day-to-day activities and finally information about your likes and dislikes. The Trust keeps an electronic copy which can be updated and provides you with a copy for you to keep with you during your stay.

The purpose is to support your care and to provide our staff with information about yourself and your carers during a hospital visit. You are not required to have a passport if you do not want one and so we use your explicit consent to hold and process the data needed for the passport.

You can withdraw your consent at any time but we could then no longer support your passport and this may affect our ability to reduce the stress of your visits.

Improving care through research

As an NHS organisation we use personally-identifiable information to conduct research to improve health, care and services. As a publicly-funded organisation, we have to ensure that it is in the public interest when we use personally-identifiable information from people who have agreed to take part in research. This means that when you agree to take part in a research study, we will use your data in the ways needed to conduct and analyse the research study. Your rights to access, change or move your information are limited, as we need to manage your information in specific ways in order for the research to be reliable and accurate. If you withdraw from the study, we will keep the information about you that we have already obtained. To safeguard your rights, we will use the minimum personally-identifiable information possible.

Health and care research should serve the public interest, which means that we have to demonstrate that our research serves the interests of society as a whole. We do this by following the UK Policy Framework for Health and Social Care Research.

Any research involving patients has to be approved by the Health Research Authority. If any research involves processing your personal data, you will usually be contacted to see if you are willing to take part. Research will only use your data without contacting you if it has been formally approved under s251 of the National Health Service Act 2006 and the and the Health Service (Control of Patient Information) Regulations 2002. S251(12) specifically refers to medical research. The Health Research Authority publishes details of such approvals and you can find a list here. The National Data Opt-Out (see below) applies to most of these approvals. If you do ask for this opt-out to apply the Trust may still contact you to invite you to partipate in specific studies. You would not be identified personally in any published results, unless you agreed to this.

When you agree to take part in a research study, the information about your health and care may be provided to researchers running other research studies in this organisation and in other organisations. These organisations may be universities, NHS organisations or companies involved in health and care research in this country or abroad. Your information will only be used by organisations and researchers to conduct research in accordance with the Policy Framework.

Your information could be used for research in any aspect of health or care, and could be combined with information about you from other sources held by researchers, the NHS or government.

Where this information could identify you, the information will be held securely with strict arrangements about who can access the information. The information will only be used for the purpose of health and care research, or to contact you about future opportunities to participate in research. It will not be used to make decisions about future services available to you, such as insurance.

Once you have agreed to take part in a research project, or that your personal data may be used for research the Trust has a clear legal basis for using your personal data as set out in the next paragraphs under Article 6.1 (e) GDPR as research is recognised to be task carried out in the public interest.

The NHS has a statutory framework which provides a clear legal basis for research in the public interest. This is set out in:

- The Health and Social Care Act 2008 (Regulated Activities) Regulations 2014 under which NHS providers have legal duties to "improve the quality and safety of the services provided" and "assess, monitor and mitigate the risks relating to the health, safety and welfare of service users" under.
- s14R NHS Act 1996 - where research is commissioned by a Clinical Commissioning Group under the duty to secure "continuous improvement in the quality of services provided to individuals for or in connection with the prevention, diagnosis or treatment of illness"
- The NHS Constitution (July 2015) made under s1 Health Act 2009 which NHS bodies must have regard to (s2). It includes a commitment, in the third of its seven guiding principles, to " … innovation and to the promotion, conduct and use of research to improve the current and future health and care of the population." The handbook to the Constitution refers specifically to the duties on the Secretary of State, NHS England and CCGs to secure continuous improvement in the quality of outcomes achieved by health services and in this context says: "The importance of innovation and medical research is underscored by this Principle as integral to driving improvements in healthcare services for patients."
- Paragraph 13 of Schedule 1 of the NHS Act 2006 as amended by the Health and Social Care Act 2012 provides that "The Secretary of State, the Board or a clinical commissioning group may conduct, commission or assist the conduct of research into— (a) any matters relating to the causation, prevention, diagnosis or treatment of illness". This includes "power to do so by providing financial assistance or making the services of any person or other resources available".

- s13L NHS Act 2006 gives the NHS Commissioning Board a duty to "promote research on matters relevant to the health service". Clinical Commissioning Groups have a similar duty under s14Y.
- s66 Health and Social Care Act 2012 requires Monitor to have regard to "the need to promote research into matters relevant to the NHS by persons who provide health care services for the purposes of the NHS".
- s72 NHS Act 2006 under which Foundation Trusts and other NHS bodies must co-operate with other NHS bodies in exercising their functions.

Most research requires the use of special category data including health information so the Trust also relies on the above legal bases together with Article 9.2 (j) of GDPR - processing is necessary for … scientific or historical research purposes.

For further information about how the NHS looks after your information when used for research please refer to the NHS Health Research Authority webpage.

If you would like to actively be involved in a research study, you may find the 'Patient and Public Involvement' page of the Trusts website useful or you can discuss the issue with your Health Care Professional.

Overseas Visitors

Where the Trust treats you as an overseas patient in addition to the above the Trust may collect additional information to establish your eligibity for free treatment within the NHS and to recover payment from you if that becomes necessary..

This may include:

- additional identification such as a passport
- proof of residence
- asylum status
- evidence of health insurance
- purpose and length of stay

Once we have satisfactorily established your status we will not retain copies of amy supporting documents you supplied.

Relevant information may be shared with the Home Office where required by the National Health Service (Charges to Overseas Visitors) Regulations 2015 so that they can confirm your immigration status to us. This will not include clinical information about your healthcare with us.

The information provided may be used and retained by the Home Office for its functions, which include enforcing immigration controls overseas, at the ports of entry and within the UK. The Home Office may also share this information with other

law enforcement and authorised debt recovery agencies for purposes including national security, investigation and prosecution of crime, and collection of fines and civil penalties.

If you are chargeable but fail to pay for NHS treatment for which you have been billed, it may result in a future immigration application to enter or remain in the UK being denied. Necessary (non-clinical) personal information may be passed via the Department of Health to the Home Office for this purpose.

National Data Opt-Out

Whenever you use a health or care service, such as attending Accident & Emergency or using Community Care Services, important information about you is collected to help ensure you get the best possible care and treatment.

The information collected about you when you use these services can also be provided to other approved organisations, where there is a legal basis, to help with planning services, improving care provided, and research into developing new treatments and preventing illness. All of these help to provide better health and care for you, your family, and future generations. Confidential personal information about your health and care is only used in this way where it is allowed by law.

You have a choice about whether you want your confidential information to be used in this way in many cases.

To find out more about the wider use of confidential personal information and to register your choice to opt out if you do not want your data to be used in this way, visit the Your NHS Data Matters website. If you do choose to opt out you can still consent to your data being used for specific purposes.

If you are happy with this use of information you do not need to do anything. You can change your choice at any time.

Trust Membership

Eligible members of the public may apply for Membership of University Hospitals Bristol NHS Foundation Trust. For details on eligibility please see the Trust Constitution, paragraph 11. For details on how to apply please see our Membership page.

If you become a Member, the Trust will keep details of your name address and date of birth (and optional email address and phone number) in order to fulfil its duties under s30 and Schedule 7 of the National Health Services Act 2006. In addition, but only with your consent the Trust may ask for details of your gender, ethnicity, whether you have a disability and for information about your interests to assist it in ensuring that membership is representative of the communities it serves.

The Trust will keep this information for as long as you are a member. You may resign your membership at any time by contacting the membership office via email foundationtrust@uhbristol.nhs.uk or by calling 0117 34 23764.

By law we are required to make a register of our membership available to the public on request. This register shows the member's name and their membership type, but not their address or any other personal details. If you wish to be taken off the public register, please get in touch with the membership office.

Job Applicants

This section of our Privacy Notice applies to prospective, current & former employees, applicants, volunteers, trainees, apprentices & those carrying out work experience. Not all of the information referred to will be relevant to some of these roles.
If you are a student on placement with the Trust please see your college's privacy notice which will explain what information is shared with the Trust for the purposes of your placement.

The Trust is the data controller for the information you provide during a recruitment process unless otherwise stated. If you have any queries about the process or how we handle your information please contact us at jobs@UHBristol.nhs.uk.

What will we do with the information you provide to us?

All of the information you provide during the process will only be used for the purpose of progressing your application, or to fulfil legal or regulatory requirements if necessary.We will not share any of the information you provide during the recruitment process with any third parties for marketing purposes or store any of your information outside of the European Economic Area. The information you provide will be held securely by us and/or our data processors whether the information is in electronic or physical format.

We will use the contact details you provide to us to contact you to progress your application. We will use the other information you provide to assess your suitability for the role you have applied for and to determine your eligibility to work in the United Kingdom.

What information do we ask for, and why?

We do not collect more information than we need to fulfil our stated purposes and will not retain it for longer than is necessary.

The information we ask for is used to assess your suitability for employment. You don't have to provide everything we ask for but it might affect your application if you don't.

Application stage

If you use our online application system, this will be collected by a data processor on our behalf (please see below).

We ask you for your personal details including name and contact details. We will also ask you about your previous experience, education, training, referees and for answers to questions relevant to the role you have applied for. Our recruitment team will have access to all of this information.

You will also be asked to provide equal opportunities information including gender, race, ethnic origin, sexual orientation, religious or other beliefs. This is not mandatory information – if you don't provide it, it will not affect your application. This information will not be made available to any staff outside of our recruitment team, including hiring managers, in a way which can identify you. Any information you do provide, will be used only to produce and monitor equal opportunities statistics.

In addition the Trust is a "Disability Confident" scheme employer. You will be invited to provide information about any disabilities so that we can offer a guaranteed interview if you meet the essential criteria for the post.

Information may also be collected from external sources such as NHS Jobs, your professional body, current or previous employers, the Disclosure and Barring Service, or government bodies like HM Revenue and Customs, the Department for Work and Pensions, or the UK Visas and Immigration.

Shortlisting

Our hiring managers shortlist applications for interview. They will not be provided with your name or contact details or with your equal opportunities information if you have provided it. "Disability Confident" information may be presented to the lead short-lister before they make the final decision on who to invite to interview.

Assessments

We might ask you to participate in assessment days; complete tests or occupational personality profile questionnaires; and/or to attend an interview – or a combination of these. Information will be generated by you and by us. For example, you might complete a written test or we might take interview notes. This information is held by the Trust.

In some cases where we think it appropriate for the role we may look at any job related profiles you may have on public social media sites such as LinkedIn, Facebook or posts you have made on public services such as Twitter.

Conditional offer

If we make a conditional offer of employment we will ask you for information so that we can carry out pre-employment checks. You must successfully complete pre-employment checks to progress to a final offer. We are required to confirm the identity of our staff, their right to work in the United Kingdom and seek assurance as to their trustworthiness, integrity and reliability.

You will therefore be required to provide:

- Proof of your identity – you will be asked to attend our office with original documents, we will take copies.
- Proof of your qualifications – you will be asked to attend our office with original documents, we will take copies.
- You will be asked to complete a criminal records declaration to declare any unspent convictions.

We will provide your email address to the Government Recruitment Service who will contact you to complete an application for any required Criminal Record check via the Disclosure and Barring Service, which will verify your declaration of unspent convictions.

We will contact your referees, using the details you provide in your application, directly to obtain references

We will also ask you to complete a questionnaire about your health. This is to establish your fitness to work. This is done through the Avon Partnership NHS Plus Occupational Health Service (APOHS). The Trust is data controller for APOHS but health data provided to them remains confidential and will not be disclosed to anyone else without your consent other than to confirm your fitness for work. For further details see Occupational Health section of this Privacy Notice.

If we make a final offer, we will also ask you for the following, either before or after you start:

- Bank details – to process salary payments
- Emergency contact details – so we know who to contact in case you have an emergency at work
- Membership of an NHS Pension scheme – so we can send you a questionnaire to determine whether you are eligible to re-join your previous scheme.

Post start date

Senior Staff may be required to declare if they have any potential conflicts of interest. If you complete a declaration, the information will be held on your personnel file.

A “fit and proper person” enquiry may be made with Experian for appointments at Executive level. Please see Experian’s Privacy Policy .

How long is the information retained for?

If you are successful, the information you provide during the application process will be retained by us as part of your employee file for the duration of your employment plus 10 years following the end of your employment.

If you are unsuccessful at any stage of the process, the information you have provided until that point will be retained for 400 days from the date of your application.

Information generated throughout the assessment process, for example interview notes, is retained on your employment file for successful candidates. For unsuccessful candidates the information is retained for the purposes of providing feedback if required but in any event for no more than six months after the interview.

Equal opportunities information is retained for six months following the closure of the campaign whether you are successful or not.

Trac Systems Ltd

If you use our online application system, you will provide the requested information to Trac Systems Ltd, who provide this online service for us. Once you click ‘Apply Online Now’ you will be taken to Trac’s website and they will hold the information you submit but the Trust will have access to it.

You can view the Trac Privacy Policy here.

Employees

As an employer, the Trust needs to keep and process information about you for normal employment purposes. The information we hold and process will be used for our management and administrative use. We will keep and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, whilst you are working for us, at the time when your employment ends and after you have left. This includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of the Trust and protect our legal position in the event of legal proceedings. If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision.

Much of the information we hold will have been provided by you, but some may come from other internal sources, such as your manager or people you work with, or in some cases, external sources, such as referees, a Trades Union, or a professional

organisation such as the British Medical Association, or one of the medical Royal Colleges.

The sort of information we hold includes your application form and references, your contract of employment and any amendments to it; correspondence with or about you, for example letters to you about a pay rise or, at your request, a letter to your mortgage company confirming your salary; information needed for payroll, benefits and expenses purposes; your hours worked, contact and emergency contact details; records of holiday, sickness and other absence; information needed for equal opportunities monitoring policy; and records relating to your career history, such as training records, appraisals, other performance measures and, where appropriate, disciplinary and grievance records.

For the purposes of security, network and application integrity, and ensuring the effective management of IT many applications will maintain logs of usage which may identify users either directly or indirectly. All internet usage is logged and internet and email traffic is monitored as detailed in our policies available in the staff handbook or on the intranet. This data may be analysed on an aggregate basis without identifying individuals for diagnostic, utilisation and planning requirements. Use of the data in a way which identifies individuals will only be authorised where this is necessary for legitimate purposes and in accordance with policies and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

You will, of course, inevitably be referred to in many Trust documents and records that are produced by you and your colleagues in the course of carrying out your duties and the business of the Trust.

Your contact details will be made available to the Trust Membership Office as employees are automatically invited to become Members of the Trust. You may opt-out of membership if you wish in accordance with Article 9 of the Trust Constitution. If you wish to opt out please contact the membership office via email foundationtrust@uhbristol.nhs.uk or call 0117 34 23764. By law we are required to make a register of our membership available to the public on request. This register shows the member's name and their membership type, but not their address or any other personal details. If you wish to be taken off the public register, please get in touch with the membership office.

Where necessary, we may keep information relating to your health, which could include reasons for absence, certificates and GP reports and notes. This information will be used in order to comply with our statutory health and safety and occupational health obligations – to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate. We will also need this data to administer and manage statutory and Trust sick pay. Occupational health

records will be kept separate and confidential from other employee records – see Occupational Health.

Where we process special categories of information relating to your racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, biometric data or sexual orientation, we will always obtain your explicit consent to those activities unless the processing is necessary for the purpose of the employment contract or required by law or the information is required to protect your health in an emergency. We will tell you whether providing the information is optional or mandatory.

In particular some staff, including staff in Hotel Services, will be required to provide biometric fingerprint data (but not a fingerprint as such) for clocking purposes. This is used in managing rostering, time and attendance records, absences, skills management and related functions.

In most cases we will be processing your data because it is necessary for the purpose of the employment contract or required by law but where we are processing data based on your consent, you have the right to withdraw that consent at any time. Occasionally we will process staff data as we have a legitimate interest in doing so – for example in relation to running the Recognising Success Awards.

Other than as mentioned below, we will only disclose information about you to third parties with your consent, if we are legally obliged to do so, or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information to a pension scheme.

In particular information may be disclosed to:

- Suppliers contractors partners and other organisations in the normal course of your employment activities – for example your contact details will be shared with anyone you correspond with, relevant personal details may be shared as part of a due diligence process where the Trust is entering into a contract or research partnership. You will normally be aware of this as part of your work. If it is something you would not reasonably expect we will let you know before doing so.
- training providers. Where the Trust commissions training on your behalf from an external supplier the Trust will share necessary information about you with the provider for the management co-ordination and quality control of that training
- HM Revenue and Customs for the administration of tax and national insurance
- professional registration organisations - e.g. in respect of fitness to practice hearings

- NHS Pensions if you are a member of the scheme
- banks & insurance companies. at your request - e.g. to confirm employment details in respect of loan/mortgage applications/guarantees
- the Department of Work and Pensions e.g. in relation to benefits enquiries
- the Child Support Agency
- the Disclosure and Barring Service
- the Student Loans Company
- the Home Office Visa & Immigration Service
- the National Clinical Assessment Service where a request is made to issue a Healthcare Professional Alert Notice as under the Healthcare Professional Alert Notices Directions 2006
- the public under the Freedom of Information Act where this does not breach the data protection principles e.g. requested names or contact details of senior managers or doctors or those in public-facing roles
- professional examination boards, including your contact details, courses and examinations where the Trust is supporting you to pursue qualifications as part of your continuing development and education

National Fraud Initiative (NFI)

The Trust is required by law to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud.

The Cabinet Office conducts data matching exercises to assist in the prevention and detection of fraud as part of its responsibility for public sector efficiency and reform. Part 6 of the Local Audit and Accountability Act 2014 enables the Cabinet Office to process data as part of the NFI.

The Trust is a mandatory participant of the NFI which is a data matching exercise undertaken by the Cabinet Office to assist in the prevention and detection of fraud. We are required to provide particular our payroll data to the Cabinet Office for each exercise.

Data matching involves comparing sets of data, such as payroll of a body against other records held by the same or another body to see how far they match. This is usually personal information and Trust creditors' data. The data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it may indicate that there is an inconsistency which requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

The Trust's legal basis to process this data is set out in Article 6 (c) of the General Data Protection Regulation (GDPR) "processing is necessary for compliance with a legal obligation to which the controller is subject;"

For further information see the Cabinet Office Privacy Notice.

For further information on data matching at University Hospitals Bristol NHS Foundation Trust contact Elias Hayes, Local Counter Fraud Specialist on 01173 420828 or elias.hayes@nhs.net.

The Trust may use data processors to hold information in files e.g. archive storage companies.

We will not normally transfer your information outside of the EEA or to an international organisation but may do so with your explicit consent e.g. where a doctor is participating in a multi-national research project.

We have in place appropriate safeguards to ensure the security of your data in accordance with the Trust's Information Security Policy.

Your personal data will kept up to date and accurate during your employment and will be retained for a minimum for a period of TBC years after the end of your employment.

If in the future we intend to process your personal data for a new purpose we will provide you with information on that purpose and any other relevant information.

Please also see information regarding Your Rights. Some of these will be of limited application, particularly during the period you remain employed. For example we would not delete records we need to comply with our statutory and contractual duties.

Occupational Health

The Trust provides occupational health advice and services to its staff and managers through the Avon Partnership NHS Plus Occupational Health Service (APOHS). APOHS is a partnership between the Trust, North Bristol NHS Trust, and Weston Area Health Authority. APOHS provides a number of services for the Trust and its staff and in particular, where required, will assist the Trust in making sure reasonable adjustments are made for staff with a disability

The partners are joint data controllers for your personal data where you have engaged with APOHS. APOHS provides a confidential medical service and will not share your information with the Trust or its managers in a way which breaches your confidentiality. For further information on how APOHS processes and looks after your information see their website.

Agency Workers

When you accept a position with the Trust as an agency worker we receive and hold information from your agency to verify your eligibility to work and suitability for the post and to manage your time with the Trust including:

- Contact details & photo ID
- References
- Employment checks such as disclosure & barring service, occupational health, and employment history
- Relevant training history

This information will be retained for up to six months following completion of your assignment in case you apply for another position during that time.

Apprentices

When you join University Hospitals Bristol NHS Foundation Trust (the Trust) as an apprentice we collect personal data about you including your contact details, date of birth, UK Unique Learner Number (supplied by you or the Department for Education) and past education. We will maintain records of your attendance, progress, tests and training. We may collect information about your health and any disabilities particularly where this is required to support you. With your consent we may collect information about your ethnicity for monitoring our duties to provide equal opportunities. Much of the general information in the "Working for Us" section of this Privacy Notice will apply to apprentices and you should read through the other sections.

We use your information generally to manage your apprenticeship, commission training, monitor your progress, manage your funding and for general employment purposes. We generally hold and use your information because it is necessary for the purposes of your apprenticeship contract. Where this does not apply we will obtain your specific consent.

Your information may also be shared with training providers and as follows:

Education and Skills Funding Agency (ESFA)

We will share information about you with the Education and Skills Funding Agency (ESFA), an executive agency of the Department of Education (DfE), to enable them to exercise their functions and to meet their statutory responsibilities, including under the Apprenticeships, Skills, Children and Learning Act 2009 and to create and maintain a unique learner number (ULN) and a personal learning record (PLR). Your information will be securely destroyed after it is no longer required for these purposes. and to allow us to claim funding. We will also provide relevant information to their Learning Records Service (LRS).

Your information may be shared by ESFA with third parties for education, training, employment and well-being related purposes, including for research. This will only

take place where the law allows it and the sharing is in compliance with data protection legislation. The English European Social Fund Managing Authority (or agents acting on its behalf) may contact you in order for them to carry out research and evaluation to inform the effectiveness of training.

Further information about use of and access to your personal data, and details of organisations with whom ESFA regularly share data, are available from their Privacy Notice and the LRS Privacy Notice.

We process your data using Maytas, a Learning Management Solution provided by Tribal. Information on Maytas may be shared with and accessed by ESFA and by Ofsted to let them check your progress and the Trust's accountability as a training provider.

Surveillance Cameras (CCTV & Body Worn Video)

We employ surveillance cameras (CCTV and Body Worn Video) in and around our hospital sites, as we have a legitimate interest in doing so, in order to:

- protect staff, patients, visitors and Trust property
- apprehend and prosecute offenders, and provide evidence to take criminal or civil action in the courts
- provide a deterrent effect and reduce unlawful activity
- help provide a safer environment for our staff
- assist in traffic management and car parking schemes
- monitor operational and safety related incidents
- help to provide improved services, for example by enabling staff to see patients and visitors requiring assistance
- assist with the verification of claims

You have a right to request surveillance information recorded of yourself and ask for a copy of it. Please see the section on Your Rights. You would need to provide sufficient information to identify you and assist us in finding any images on our systems.

We reserve the right to withhold information where permissible by Data Protection Legislation 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 or Body Worn Video data for legal reasons. When this is done there is a requirement for the organisation that has received the images to adhere to Data Protection Legislation.

Your Rights and Subject Access Requests

Data Protection law gives you significant rights over the use of your personal data. The most important is the right to make a "Subject Access Request" for access to the information we hold, usually by being provided with a copy. Further details are provided below. Your other rights include:

- Rectification: a right to ask us to change any personal data which is wrong
- Erasure: a right to ask us to delete any personal data we hold. This is sometimes referred to as “the right to be forgotten”
- Restriction: a right to ask us not to process your information for certain purposes. There is also a specific right to ask us not to use your contact details for marketing purposes.
- Objection: a right to object to some types of processing based on your own individual circumstances
- Data portability: the right to receive your information in a specific form so that it can be used by another organisation. However this right usually only applies where we are processing information by consent so it does not apply to medical records. For more information please see the Information Commissioner’s website.

These rights are not absolute (other than prevention of marketing) and will not apply in all circumstances. For example, you do not have a right to insist that we delete your medical records as we have a legal duty to keep them.

For more information about your rights please see the ICO's guide to individual rights.

If you wish to exercise any of the rights other than a Subject Access Request please contact the Trust's Data Protection Officer via post at Trust Headquarters, Marlborough Street, Bristol, BS1 3NU, email InformationGovernance@UHBristol.nhs.uk or by phone at 0117 342 3701.

You also have a right to complain to the Information Commissioner if you are in any way unhappy with the way we have processed your personal information or allowed you to exercise your rights. Please see: www.ico.org.uk/concerns .

Subject Access Requests

GDPR gives you the right to access the information we hold about you on our records.

For medical records requests should be made in writing to the Medical Records Department. The Trust will provide the information to you within one month of receipt of your request and sufficient information to identify you.

There is generally no charge but the Trust reserves the right to make a reasonable administrative charge in the case of requests which are manifestly unfounded or excessive, in particular because of their repetitive character.

It is possible for you to make requests on behalf of children you are responsible for and in some cases for adults e.g. where you have their specific authority or a Power of Attorney or they are incapable of making their own request.

Further information can be found here. To make a request relating to information shared with Connecting Care please follow this link.

You can also find useful information about exercising your right of access and what you can expect here.

Rectification

If you think that the data we hold on you is inaccurate or incomplete you may ask us to rectify or complete it. You can make your request by contacting the Trust's Data Protection Officer at the above address, by email to InformationGovernance@UHBristol.nhs.uk or by phone at 0117 342 3701. We will tell you within one month what action we intend to take in response to your request.

Erasure

Under GDPR you sometimes have a right to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. You can make your request by contacting the Trust's Data Protection Officer at the above address, by email to InformationGovernance@UHBristol.nhs.uk or by phone at 0117 342 3701. We will tell you within one month what action we intend to take in response to your request.

However this right does not apply to many of our key data holdings such as health records and employees' records as we are keeping such records as part of our legal duties. For a full explanation of the right and when it applies please see the Information Commissioner's website.

Restriction

These is closely linked to other rights. You have the right to restrict processing in limited circumstances for example if you think our data is inaccurate and you want to limit what we do with it until we have considered rectification (see above). You can make your request by contacting the Trust's Data Protection Officer at the above address, by email to InformationGovernance@UHBristol.nhs.uk or by phone at 0117 342 3701. We will tell you within one month what action we intend to take in response to your request.

Objection

You have a general right to object to our processing your personal data if we are processing your information for direct marketing. We will always respect such an objection.

You also have a right to object on “grounds relating to your particular situation” when we are processing your personal data:

- On the basis of our legitimate interests or the performance of a task in the public interest/exercise of official authority. This would include our processing of medical records and employee records; or
- For purposes of scientific/historical research and statistics.

For example, someone might object to us sharing identifying or address information if they were on a witness protection program. We can refuse to uphold an objection, if it is not based on their particular situation or in any event on compelling grounds – for example to save the life of a child of the person on the witness protection program.

You can make your request by contacting the Trust’s Data Protection Officer at the above address, by email to InformationGovernance@UHBristol.nhs.uk or by phone at 0117 342 3701. We will tell you within one month what action we intend to take in response to your request.

For a full explanation of the right and when it applies please see the Information Commissioner’s website.