University Hospitals Sussex NHS Foundation Trust Privacy Notice for Employees

This privacy notice tells you what to expect us to do with your personal information in order to manage your employment with the Trust.

You can find more detailed information about how we use your information for the following specific purposes here:

- The Trust's general Privacy Notice can be found at (https://www.uhsussex.nhs.uk/resources/your-personal-information/)

Our contact details

Name: University Hospitals Sussex NHS Foundation Trust

Address: Worthing Hospital Lyndhurst Road Worthing West Sussex BN11 2DH

General phone number: 01903 205111

General inquiries email address: https://www.uhsussex.nhs.uk/contact/

Website: https://www.uhsussex.nhs.uk/

We are the controller for your information. A controller decides on why and how information is used and shared.

Data Protection Officer contact details

Our Data Protection Officer is Head of Information Governance and is responsible for monitoring our compliance with data protection requirements. You can contact them with queries or concerns relating to the use of your personal data at:

Head of Information Governance/Data Protection Officer

Information Governance Team
University Hospitals Sussex NHS Foundation Trust
Worthing Hospital
Lyndhurst Road
Worthing
West Sussex
BN11 2DH

Email: uhsussex.informationgovernance@nhs.net

How do we get information and why do we have it?

The personal information we collect is provided directly from you for the following reasons:

- you have applied for a job with us or work for us.
- you have made a complaint.

We also receive personal information about you indirectly from others, in the following scenarios:

- from other health and care organisations involved in your care so that we can provide you with care
- from family members or carers to support your care

What information do we collect?

Personal information

We currently collect and use the following personal information:

- basic details about you – name, address, date of birth, next of kin and GP.
- additional contact information such as telephone numbers (home and/or mobile) and email address
- details of your skills, qualifications, employment history, experience, and professional membership (if relevant), and training history
- pre-employment checks, including referees.
- your nationality and immigration status, to confirm your eligibility to work in the UK.
- your national insurance number, tax, and bank details
- details of your pension
- remuneration, including salary and entitlement to benefits.
- photographic identity (for example, photographs for ID badges or our website)

More sensitive information

We process the following more sensitive data (including special category data):

- information about medical or health conditions, including whether you have a disability for which the organisation needs to make reasonable adjustments.
- equal opportunities monitoring information, including information about your ethnic origin, sexual orientation, health and religion or belief.
- biometric data (where used for identification purposes)
- data concerning trade union membership.
- data relating to criminal or suspected criminal offences.

Who do we share information with?

We may share information with other organisations including:

- In order to enable effective staff administration and comply with our obligations as your employer, we will share the information which you provide during the course of your employment (including the recruitment process) with the NHS Business Services Authority for maintaining your employment records, held on systems including the national NHS Electronic Staff Record (ESR) and Care Information Services (smartcard) Systems.
- 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.
- Third party companies who process staff data on behalf of the Trust including payroll and pensions processing and occupational health services.

- 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. HMRC, 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 collaborate 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)
- National Fraud Initiative (NFI) - a data matching exercise conducted by the Cabinet Office under its data matching powers as set out in Part 6 of the Local Accountability and Audit Act 2014
- 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.

We may also process your information to de-identify it, so that it can be used for purposes beyond maintaining your employment records, whilst maintaining your confidentiality. These purposes will include to comply with the law and for public interest reasons.

Employee Monitoring

The Trust's Informatics Department is committed to maintaining the privacy, dignity, and confidentiality of service users at all times. We adhere to the principles of data protection legislation, Department of Health and NHS Digital policies, procedures, and codes of practice.

The Informatics Department uses your personal information to create and manage IT user accounts, monitor system access and performance.

System generated audit trails are also used to improve internal processes, identify account and system issues, and establish if inappropriate access and/or use of IT equipment/resources have occurred.

Audit trails may also be released to patients requesting details of employees who have accessed their medical record.

External IT Monitoring

NHS Digital now provides national monitoring of all internet activity through NHS devices to local organisations such as hospitals and GP surgeries. This means that all internet activity is monitored to quickly identify any abnormalities so that immediate action can be taken to address any potential problem as quickly as possible. NHS Digital will be able to identify the affected device and user in real time so that alerts can be provided nationally and locally to minimise the threat to the NHS, staff, and patients.

The UHSussex process will be that whenever an alert is received Informatics will immediately retrieve the device and commence erasing any data and rebuilding the device, please be aware that any information stored locally on the machine will be removed with immediate effect.

Appropriate action will be taken over any inappropriate or malicious breaches detected in line with the Trust policies and procedures.

Registration Authority Smartcards

If you hold or register for an NHS Registration Authority (RA) Smartcard your personal information including your driving license and passport numbers may be recorded along with a photographic image within the NHS Digital's Care Identity Service (CIS) System.

All users issued with a Smartcard can update certain aspects of their record on the CIS database as well as change their pin code and, when necessary, renew their own Smartcard certificates. (Certificates last two years and can be self-renewed within 90 days leading to the expiry date – after this time please contact your local Registration Authority).

All personal and sensitive information is treated as sensitive ('special category') personal data, in respect of data protection legislation and can be shared by the recipient only, with the individual's consent and with others who have a legitimate need to know.

Your information may be released without your knowledge or consent in exceptional circumstances dictated in the professional codes of ethical behaviour and statute law i.e. the prevention and detection of a serious crime, fraud, malpractice allegation, court order or the vital interests of yourself or another (life or death).

NHS Mail

The Trust uses the NHS Mail email system as our main communication system. As a member of staff, you are accepting you will work within the NHSmail Acceptable Use Policy. This occurs when you register for the service. This is your promise to all NHSmail users and the public and patients we serve, that you will be mindful of the importance of the information that they share over NHSmail.

Information is stored in the NHSmail service for a variety of reasons and is retained in accordance with their policies. The NHSmail Data Retention and Information Management Policy defines the scope of data held and details the recovery of data. The process to request this is available in the NHSmail Access to Data Policy on the NHSmail portal help pages.

Responsibilities for data protection are explained in the Transparency Information document located within the General Data Protection Regulation section of the NHSmail portal help pages.

Is information transferred outside the UK?

University Hospitals Sussex NHS Foundation Trust do not routinely transfer information outside the European Union.

Where there is a need to transfer information outside the UK or European Union, we will ensure that the security and protections that are put in place are of equivalent standard to those standards that we would use within the UK or European Union when processing your information.

What is our lawful basis for using information?

Personal information

Under the UK General Data Protection Regulation (UK GDPR), the lawful basis we rely on for using personal information is:

(b) We have a contractual obligation - between a person and a service, such as a service user and privately funded care home.

(c) We have a legal obligation - the law requires us to do this, for example where NHS England or the courts use their powers to require the data.

More sensitive data

Under UK GDPR, the lawful basis we rely on for using information that is more sensitive (special category):

(b) We need it for employment, social security, and social protection reasons (if authorised by law). See this list for the most likely laws that apply when using and sharing information in health and care.

(h) To provide and manage health or social care (with a basis in law). See this list for the most likely laws that apply when using and sharing information in health and care.

Common law duty of confidentiality

In our use of health and care information, we satisfy the common law duty of confidentiality because:

- you have provided us with your consent (we have taken it as implied to provide you with care, or you have given it explicitly for other uses)
- we have support from the Secretary of State for Health and Care following an application to the Confidentiality Advisory Group (CAG) who are satisfied that it isn't possible or practical to seek consent
- we have a legal requirement to collect, share and use the data.
- for specific individual cases, we have assessed that the public interest to share the data overrides the public interest served by protecting the duty of confidentiality (for example sharing information with the police to support the detection or prevention of serious crime). This will always be considered on a case-by-case basis, with careful assessment of whether it is appropriate to share the information, balanced against the public interest in maintaining a confidential health service.

How do we store your personal information?

Your information is securely stored for the time periods specified in the Records Management Code of Practice. We will then dispose of the information as recommended by the Records Management Code for example we will:

- securely dispose of your information by shredding paper records or wiping hard drives to legal standards of destruction.

- archive historically significant information at the West Sussex Record Office

What are your data protection rights?

Under data protection law, you have rights including:

Your right of access - You have the right to ask us for copies of your personal information (known as a subject access request).

Your right to rectification - You have the right to ask us to rectify personal information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete.

Your right to erasure - You have the right to ask us to erase your personal information in certain circumstances.

Your right to restriction of processing - You have the right to ask us to restrict the processing of your personal information in certain circumstances.

Your right to object to processing - You have the right to object to the processing of your personal information in certain circumstances.

Your right to data portability - You have the right to ask that we transfer the personal information you gave us to another organisation, or to you, in certain circumstances.

Automated decision-making including profiling

- **Automated decisions**

  This is called automated decision making and profiling for example, completing an online aptitude test using a pre-programmed algorithm and or criteria when applying for a job vacancy with the hospital.

  You can ask for information to understand the reasons behind the automated decisions. The request can be made verbally or in writing. We recommend that you follow up any verbal requests in writing by contacting the Trust's Data Protection Officer explaining your request.

- **Profiling**

  Profiling means information about you is used to analyse or predict things like:

  - The risks associated with a medical condition.
  - Computerised analysis of MRI scans to improve a patient's diagnosis and recovery performance at work
  - Your personal financial status
  - Your health, personal preferences, and interests.

  You can object to the collection of profiling information if it includes direct marketing.

You are not required to pay any charge for exercising your rights. If you make a request, we have one month to respond to you.

Please contact us at uhsussex.informationgovernance@nhs.net if you wish to make a request.

How do I complain?

If you have any concerns about our use of your personal information, you can make a complaint to us at

uhsussex.informationgovernance@nhs.net

Telephone: 07900736922

C/O Information Governance Department
University Hospitals Sussex NHS Foundation Trust
Worthing Hospital
Lyndhurst Road
Worthing
West Sussex
BN11 2DH

Following this, if you are still unhappy with how we have used your data, you can then complain to the ICO.

The ICO's address is:

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

Helpline number: 0303 123 1113

ICO website: https://www.ico.org.uk

Date of last review

11th June 2025