

University Hospitals Sussex NHS Foundation Trust Privacy Notice for Overseas Patients and Patients Not Ordinarily Resident in the UK

This privacy notice tells you what to expect us to do with your personal information when you contact us or use our services.

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 provided information to seek care – this is used directly for your care, and to manage the services we provide, to clinically audit our services, investigate complaints, or to be used as evidence as part of an investigation into care.
- 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.
- Establish your identity and your entitlement to free NHS treatment.
- Record outstanding NHS debts and provide this to the Department of Health & Social Care
- Determine your immigration status using Home Office services.
- Prevent, detect, and prosecute fraud and other crime.
- Provide translation and interpretation services.

More sensitive information

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

- data concerning physical or mental health (for example, details about your appointments or diagnosis)
- data revealing racial or ethnic origin.
- data concerning a person's sex life.
- data concerning a person's sexual orientation.
- genetic data (for example, details about a DNA sample taken from you as part of a genetic clinical service)
- biometric data (where used for identification purposes)
- data revealing religious or philosophical beliefs.
- data relating to criminal or suspected criminal offences.

Who do we share information with?

We may share information with other organisations including:

- other hospitals and community organisations (e.g. community care teams, care homes etc.) providing care services.
- planners of health and care services (such as Department of Health, Integrated Care Boards)
- specialist companies providing diagnostic and testing services you might need.
- those with parental responsibility for patients, including guardians.
- carers without parental responsibility (subject to explicit consent)

- medical researchers for research purposes (subject to explicit consent, unless the data is anonymous)
- bodies with statutory investigative powers such as the Care Quality Commission, the General Medical Council, the Health and Safety Executive, the Parliamentary and Health Service Ombudsman National generic registries, for example the UK and Ireland Association of Cancer Registries
- third party data processors (such as IT systems suppliers)
- solicitors, the police, the courts (including a Coroner's court), debt recovery agencies, tribunals, and enquiries.
- Government agencies or public bodies within your home country
- companies that provide translation services and with whom we have a contract.
- medical insurers for the purposes of administration of a claim for payment of medical expenses

In some circumstances we are legally obliged to share information. This includes:

- when required by NHS England to develop national IT and data services
- when registering births and deaths
- when reporting some infectious diseases
- when a court orders us to do so
- where a public inquiry requires the information

We will also share information if the public good outweighs your right to confidentiality. This could include:

- where a serious crime has been committed
- where there are serious risks to the public or staff
- to protect children or vulnerable adults

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

Is information transferred outside the UK?

University Hospitals Sussex NHS Foundation Trust does not routinely transfer information outside the European Union but may do so if there is a need to contact a government agency in your home country, or possibly your medical insurer. Some organisations we share with, such as debt recovery agencies may transfer information outside the European Union if there is a need to do so.

Where this is the case, 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 and 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:

(e) We need it to perform a public task - a public body, such as an NHS organisation or Care Quality Commission (CQC) registered social care organisation, is required to undertake activities by law. See [this list](#) for the most likely laws that apply when using and sharing information in health and care.

More sensitive data

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

(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](#)).

How to make a request for copies or access to your information not held in my health and care record:

- **Medical records**

RSCH or Princess Royal Hospitals uhsussex.subject.access@nhs.net

Southlands, St Richard's, or Worthing Hospitals uhsussex.SAR.Worthing@nhs.net

- **X-rays and MRI scans only**

RSCH or Princess Royal Hospitals uhsussex.radiologyimageaccess@nhs.net

Worthing Hospitals Radiology.enquirieswash@nhs.net

St Richard's Hospitals Radiology.enquiriesrsh@nhs.net

- **CCTV images**

RSCH or Princess Royal Hospital drew.willis@nhs.net

Southlands, St Richard's, or Worthing Hospitals nick.rossiter@nhs.net

- **Complaints** Uhsussex.patient.experience@nhs.net

- **Current and former employees** uhsussex.employee.relations@nhs.net

- **Occupational health services** uhsussex.duty.OH@nhs.net

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.

National data opt-out

- we are applying the national data opt-out because we are using confidential patient information for planning or research purposes.

The information collected about you when you use health and care 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 lawful basis to use this information. All these uses help to provide better health and care for you, your family and future generations. Confidential health and care information is only used like this when allowed by law.

Whenever possible, data used for research and planning is anonymised, so that you cannot be identified, and your confidential information is not accessed.

You have a choice about whether you want your confidential 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 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.

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.

Use of Artificial Intelligence Technology

The Trust participates in the use of Artificial Intelligence (AI) which is the use of digital technology to create systems that can perform tasks commonly thought to require human intelligence.

AI can help a Health and Care professional to reach a decision about your care, e.g., diagnosing a condition you have or to help you in choosing treatment options.

Decisions will not be made solely by the AI system; Health and Care professionals will always review and provide you with advice, allowing you to make the final decision on the care and treatment you receive.

Examples of where AI technology is used within the Trust:

- analysing Dermoscopic images to streamline the referral process for skin cancer and direct listing for surgery where appropriate
- comprehensive interpretation of chest x-rays and CT brain scans

CCTV and BWC

Closed Circuit Television (CCTV) and Body Worn Cameras (BWC) are to assist in the prevention of crime, against persons and property and to reduce the risk of crime for Trust staff, service users and carers.

For safety and security reasons, the Trust security personnel wear BWC while on duty. Recordings will not be continuous and security staff will make an announcement if they need to turn the cameras on. To maintain privacy and dignity, recordings will not be permitted in areas of the hospital where examinations or procedures are being undertaken or if there is likely to be nudity. Anyone present may object to the recording but will need to show the need for privacy outweighs the need to protect the public.

The Trust's security services, including the use of CCTV and BWC, are managed internally.

The Trust remains the data controller of this data and any disclosures to third parties such as the Police, will only be done with the permission of the Trust.

Collaborative Working

- **Integrated Care Record (ICR)**

Health and care organisations across Sussex are working to improve the care our population receives through a wide-reaching programme of digital transformation designed to use digital technology to provide better care for local people and use our resources in a more effective and efficient way.

Part of this digital transformation programme is focusing on the development of Integrated Care Records (ICRs).

An ICR enables the different health and care organisations involved in an individual's care to access relevant information about them without the need to access multiple IT systems.

For more information, please see the [Sussex Health & Care - My Health and Care Record](#).

- **The NHS Federated Data Platform (NHS FDP)**

The NHS Federated Data Platform (NHS FDP) – is a series of separate data platforms, known as instances. University Hospitals Sussex NHS Foundation Trust has its own instance of the NHS FDP which makes it easier for health and care organisations to work together, compare data, analyse it at different geographic, demographic, and organisational levels and share and spread new effective digital solutions. The NHS FDP can connect and share information between health and care organisations when it is helpful and where legal data sharing agreements are in place. For example, to discharge a patient from hospital into a care setting.

In this Trust, the NHS FDP will be used for inpatient and outpatient care co-ordination and for the RTT (Referral to Treatment Time) validation tool. The respective privacy notices for each of these areas can be reviewed using the links below:

- [Inpatient CCS Privacy Notice](#)
- [Outpatient CCS Privacy Notice](#)
- [RTT Privacy Notice](#)

The NHS FDP is not a data collection; it is software procured by NHS England that will help to connect disparate sets of data and allow them to be used more effectively for care. If you would like to find out more about this, please visit: [NHS England » Data platform frequently asked questions](#).

- **Surrey, Sussex, and Frimley Imaging Network (SSFIN)**

The Surrey, Sussex, and Frimley Imaging Network (SSFIN) is a joint venture between:

1. Ashford and St Peter's NHS Foundation Trust (ASPH)
2. East Sussex Healthcare NHS Trust (ESHT)
3. Frimley Health NHS Foundation Trust (FHFT)
4. Queen Victoria Hospital NHS Foundation Trust (QVH)
5. Royal Surrey NHS Foundation Trust (RSFT)
6. Surrey & Sussex Healthcare NHS Trust (SASH)
7. University Hospitals Sussex NHS Foundation Trust (UHSussex)

Ashford & St Peters NHS Foundation Trust is the host organisation entering into contracts on behalf of SSFIN.

SSFIN respects your privacy and is committed to protecting your personal data.

The type of information we hold about you

In connection with providing your care, the images we take will be shared across SSFIN where we will collect, store, and use the following categories of personal and sensitive personal information about you:

- The information we receive from a clinician requesting a radiology exam for you. This includes details of your name, surname, date of birth, address, NHS number, hospital number, gender, details of the radiology exam being requested.
- The information you may provide to us in connection with the radiology exam we conduct for you.
- The results of your radiology exam (we will share the results with the requesting clinician)

Who is your personal information processed by?

We process personal information about you from the following sources:

- Clinicians requesting radiology exams for you.
- From the Partner Organisations which make up Surrey, Sussex, and Frimley Imaging Network (SSFIN):

SSFIN Organisation	Link to Privacy Notice
Ashford and St. Peter's Hospitals	https://www.ashfordstpeters.nhs.uk/
East Sussex Healthcare NHS Trust	https://www.esht.nhs.uk/
Frimley Health NHS Foundation Trust	https://www.fhft.nhs.uk/
Queen Victoria Hospital NHS Foundation Trust	https://www.qvh.nhs.uk/
Royal Surrey NHS Foundation Trust	https://www.royalsurrey.nhs.uk/
Surrey and Sussex Healthcare NHS Trust	https://www.surreyandsussex.nhs.uk/
University Hospitals Sussex NHS Foundation Trust	https://www.uhsussex.nhs.uk/
Other NHS Organisations:	
Surrey, Sussex, and Frimley GP practices	https://www.sabp.nhs.uk/
Surrey and Borders Partnership NHS FT	https://www.sabp.nhs.uk/

We share with other NHS and authorised external organisations your information for direct care when you are being treated.

How will we use information about you?

We will use the personal information we collect about you for direct care to:

- provide radiology services, which includes:
 - processing, analysing, and reporting to the requesting clinician on imaging taken.
 - providing imaging requesting and imaging delivery management tools
 - for process management and improvement
 - notifying you or your clinician about changes to SSFIN projects/ services and to otherwise manage our communications with you; and/or
 - to comply with legal and/or regulatory requirements

Why might you share my personal information with third parties?

We may disclose/ share your information with selected third parties including:

- the Partners of SSFIN (listed above)
- suppliers, sub-contractors required for the performance of any contract SSFIN entered with them, you, or your clinician.
- for the purposes of investigating any potential legal claims against SSFIN and/or any of the Partners, your information may be shared with our insurers and/or legal representatives to obtain advice and services.
- national screening or public health monitoring schemes such as Public Health England

We may also share/ disclose your personal information to third parties if SSFIN and/or any of the Partners are under a duty to disclose or share your information to comply with any legal obligation, or to deliver the radiology services in the public interest.

When we share such information, we ensure that we are only sharing as much information as it required to fulfil the purpose for which we are sharing it.

Data security

We have put in place security measures to prevent your personal information from being accidentally lost, used, or accessed in an unauthorised way, altered, or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need-to-know. They will only process your personal information on our instructions, and they are subject to a duty of confidentiality.

We have deployed technical security measures to keep your information secure when being stored or transferred electronically, this includes ensuring all security software and encryption is up to date helping to prevent the risk of cyber-attack.

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