

Privacy Notice for Your Information

What is a privacy notice?

A Privacy Notice is a statement by the Trust to patients, visitors, carers, and the public that describes how we collect, use, retain and disclose personal information that we hold about you. This privacy notice is part of our commitment to ensure that we process your personal information fairly and lawfully. This notice also explains what rights you have to control how we use your information.

The Data Protection Act and General Data Protection Regulation (GDPR) controls how your personal information is used by organisations. Under the Act, the Trust is defined as a 'data controller' of personal information that we hold. We collect information to help us provide and manage healthcare for our patients.

In order for the Trust to be able to process your information lawfully, we are obliged to satisfy a condition under Article 6 and, where special category data (sensitive information) is being processed, under Article 9 of the GDPR. The following legal bases will apply: 6(1)(e) 'for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller'; and: 9(2)(h) 'Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional'.

The trust is registered with the Information Commissioner's Office (registration number ZA030561).

The information we hold about you

We keep records about your health and any treatment and care you receive from us. This helps to ensure that you receive the best possible care from us. The information we collect normally includes:

- Name, address, date of birth, NHS number and next of kin details,
- Contacts we have had with you, such as appointments and/or home visits,
- Information about your health, such as details of diagnosis, health conditions, allergies and the treatment and care you have received,
- Relevant information from other health and social care professionals in order to support the care you receive from us.

The trust also records CCTV images for the prevention and detection of crime.

Keeping your information safe and accurate

We always keep your information securely and have strict rules about who can access it and how it can be used. We do our best to keep it accurate and up to date, so we will often check it with you when you attend one of our hospitals.

This leaflet describes the circumstances in which we may share your information with other organisations.

We have a legal duty to keep information about you confidential. We expect all our partner organisations to apply the same strict security to your records as we do, and we make sure appropriate safeguards are in place before sharing any information.

We will only share your information in strict accordance with the law, and we never use or sell it for commercial purposes.

Supporting your direct care

The Trust uses your personal information to provide healthcare to you and for purposes directly related to that healthcare (such as booking and managing appointments).

Your information may be used for clinical audit, where the team involved in your care and those working to support them will check the quality and outcomes of the treatment provided.

If you receive care from other health & social care professionals, we may share with them the information we hold about you to improve your care.

Some of the organisations that we may share with are;

- Other NHS Trusts and Foundation Trusts
- Clinical commissioning groups (who commission hospital services - usually information is partly or fully anonymised)
- General Practitioners (GP)
- Ambulance services
- Social services
- Private sector providers, such as care homes or home care delivery services
- Family, associates, and representatives (with your consent or under Lasting Power of Attorney / Deputyship under Mental Capacity Act - Personal Welfare)

In some cases, such as where we deliver a service jointly with other healthcare provider organisations, we will share information about all patients receiving that service. The department where you are being treated will be able to tell you if this applies for the particular type of care you are receiving.

Surrey Safe Care / Oracle Cerner Millennium

Royal Surrey NHS Foundation Trust and Ashford and St. Peter's Hospitals NHS Foundation Trust have a joint electronic patient record, known as Surrey Safe Care, as a replacement for their separate patient administration systems.

This means that all patient-related information, both clinical and administrative, is recorded in a joint system and is used by staff for the purpose of providing the service of direct care. Access to information follows the principle of 'need to know', using a role-based approach across user accounts. Access is additionally governed by our Confidentiality and Data Protection Policy and the Confidentiality NHS Code of Practice.

Providing a shared record improves communication over the many different clinical pathways that an individual may go through during the course of their treatment, giving clinicians access to timely information to provide the best possible care.

Supporting other medical purposes

The Trust may use information about you, and the care you have received, to improve the healthcare we provide to all patients. This includes medical research, monitoring and improving our services, and for other medical purposes where we believe there is a public benefit. If your information would be shared outside the team that provided care

to you, or those working to support them, we would first anonymise it so that you cannot be identified.

In order to improve services, we also participate in national schemes, such as patient surveys to gain feedback from patients about their experience at the Trust. These are completed voluntarily, and we may, on occasion, contact you to discuss the feedback you provided if you supplied contact details. For some surveys, the Trust employs third party services to collect and process the data. The Trust only appoints processors who can provide sufficient guarantees that the requirements of the GDPR are met and that the rights of patients are protected.

The Trust carries out audits of care, which also collect data from NHS organisations all over the country. We can normally only do this if there is a lawful basis provided by the Secretary of State for Health or the Health Research Authority, or else with your explicit consent. The department where you are being treated will be able to tell you about any national schemes for the particular type of care you are receiving.

We also use your information to ensure we are paid correctly for the services that we have delivered.

Berkshire Surrey Pathology Services (BSPS)

As part of your care, you may have provided samples e.g. urine or blood etc. which will be processed by the Trust's laboratory, or, if a specialised test, with a partner laboratory. The results of these tests and a record of the drugs you have been prescribed are stored by the Trust. The Trust is part of Berkshire Surrey Pathology Services (BSPS) which is a joint venture of Pathology Services between Ashford and St Peters, Frimley Health, Royal Berkshire, Royal Surrey NHS and Surrey and Sussex Healthcare NHS Trusts.

To view their Privacy Notice, please see:

www.berkshireandsurreypathologyservices.nhs.uk/privacy-policy/.

Your right to refuse - the National Data Opt-Out

How the NHS and care services use your information

Ashford & St Peter's Hospitals NHS Foundation Trust is one of many organisations working in the health and care system to improve care for patients and the public.

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

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

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

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

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

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

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

- See what is meant by confidential patient information
- Find examples of when confidential patient information is used for individual care and examples of when it is used for purposes beyond individual care
- Find out more about the benefits of sharing data

- Understand more about who uses the data
- Find out how your data is protected
- Be able to access the system to view, set or change your opt-out setting
- Find the contact telephone number if you want to know any more or to set/change your opt-out by phone
- See the situations where the opt-out will not apply

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

<https://www.hra.nhs.uk/information-about-patients/> (which covers health and care research); and <https://understandingpatientdata.org.uk/what-you-need-know> (which covers how and why patient information is used, the safeguards and how decisions are made)

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

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

Health and care organisations must have systems and processes in place so they can be compliant with the national data opt-out and apply your choice to any confidential patient information they use or share for purposes beyond your individual care. Our organisation is compliant with the national data opt-out policy.

What your objection covers

Your objection applies to all information held about you which is not related to your own direct care.

The Trust is required by law to report certain information to other public authorities, including notifications of births, deaths, and infectious diseases.

Other rights

Under data protection law, you have a number of very important rights, these are:

Your right of access

You have the right to ask us for copies of your personal information. This right always applies. There are some exemptions, which means you may not always receive all the

information we process. The Trust must respond within 30 calendar days. Further information can be found here: <https://www.ashfordstpeters.info/health-records>

Your right to rectification

You have the right to ask us to rectify information you think is inaccurate. You also have the right to ask us to complete information you think is incomplete. This right always applies. The Trust must respond within 30 calendar days. The Trust may refuse the request if it believes the information is accurate/complete or there is a legal basis to refuse, and you will be notified of this. To exercise your right, you should inform the organisation that you are challenging the accuracy of your data and want it corrected.

You should:

- state clearly what you believe is inaccurate or incomplete
- explain how the organisation should correct it, and
- where available, provide evidence of the inaccuracies.

Your right to erasure

You have the right to ask us to erase your personal information in certain circumstances. It should be understood that in data protection law nothing can be erased from a health record but a correction may be added and a copy given to you.

Your right to restriction of processing

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

Your right to object to processing

You have the right to object to processing if we are able to process your information because the process forms part of our public tasks or is in our legitimate interests.

Your right to data portability

This only applies to information you have given us. You have the right to ask that we transfer the information you gave us from one organisation to another or give it to you. The right only applies if we are processing information based on your consent or under, or in talks about entering into a contract and the processing is automated.

Any requests should be sent to the Trust's Data Protection Officer: asp-tr.ig@nhs.net

If you are a carer ...

If you have lasting power of attorney for health & welfare, you can make decisions on behalf of the patient. We will ask to see evidence of that power.

Otherwise, please speak to the health professional treating the patient. They will be able to make a decision based on the patient's best interests, taking your views into account.

If you are a parent ...

If you have parental responsibility for a child, you can only make decisions on their behalf until they are mature enough to understand and make an informed decision for themselves. We will normally try to seek independent consent from any child aged 12 or over, but the health professional treating them will always make a decision based on the individual child and their maturity.

In addition, you also have the right to request that the Trust corrects any personal information if it is found to be inaccurate or out of date, and also erase information if it is no longer necessary for the Trust to retain such data.

All patient records are destroyed in accordance with the Department of Health's Records Management Code of Practice for Health and Social Care 2016 (<https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016>), which sets out the appropriate length of time each type of NHS records is retained. All records are securely destroyed once their retention period has been met and the Trust has made the decision that the records are no longer required.

SMS for appointments

To keep our patients informed about appointments and to cut down on DNAs, we send information out via SMS as appointment reminders for our patients. If you do not want to receive these alerts to your mobile phone, please let us know and we will remove you from this appointment service.

SMS for Friends and Family Test (FFT)

The NHS actively encourages feedback from the public, patients and staff, and welcomes its use to improve its services. FFT is a feedback mechanism for patients to provide their feedback about their experience at the Trust. In order to gain patient feedback, we send a link to the FFT survey via SMS to patients after their appointment. If you do not wish to receive the survey via SMS to your mobile phone, please let the service know and we will remove you from this service.

Surrey Care Record

The Surrey Care Record is a local, digital shared care record for health and care professionals across Surrey Heartlands. It allows the secure sharing of your health and care data between authorised health and care professionals for the purposes of delivering safer, quicker, more personalised and more coordinated local health and care services.

Only authorised care professionals with a legitimate relationship to the care you receive will be able to access the parts of your shared care record that enable them to deliver your care. Only approved staff can log onto the Surrey Care Record and all access is logged. Please see the Surrey Care Record Privacy Notice for further detail about how personal data included in the shared care record is used and protected:

<https://www.surreyheartlands.org/surrey-care-record>

Raising a concern

Patients who have a concern about the way their records have been handled or shared should contact the Patient Advice & Liaison Service (PALS) (details below).

Additionally, patients have the right to complain to the Information Commissioner if they should ever be dissatisfied with the way the Trust has handled or shared their personal information (details below).

Further Information

For more details about how the Trust uses your information, or to discuss any concerns you may have, in the first instance please speak to the Matron, Senior Nurse or Manager on duty. If they cannot resolve your queries, please contact our Patient Experience Team on 01932 723553 or email asp-tr.patient.advice@nhs.net

Under data protection legislation the Trust is required to have a Data Protection Officer (DPO) and it is their role to:

- Inform and advise the organisation and its employees about their obligations to comply with applicable data protection legislation;
- Support and monitor compliance with applicable data protection legislation;
- Be the first point of contact for individuals whose data is being processed.

The Trust's Data Protection Officer is our Information Governance Manager, and you can contact them by:

- Email - asp-tr.IG@nhs.net
- Telephone - 01932 722 416

Further information regarding the role of the DPO and more about your rights can be found on the Information Commissioner's Office website - www.ico.org.uk

Other people with related responsibilities:

In addition to the DPO, the Trust has in place the following people with related responsibilities:

- The Director of Finance & Information acts as Senior Information Risk Owner (SIRO) and they are accountable and responsible for information risk across the organisation. They have responsibility for ensuring the organisation complies with data protection legislation and that everyone is aware of their personal responsibility to exercise good judgement, and to safeguard and share information appropriately.
- The Medical Director acts as Caldicott Guardian and they have responsibility for protecting the confidentiality of people's health and care information and making sure it is used properly. All NHS organisations must have a Caldicott Guardian.
- Information Governance Team support the above roles in discharging their data related responsibilities.

Last Updated December 2023.