

# Privacy Notice: Your personal data and how we use it



## 1. About us

Maidstone and Tunbridge Wells NHS Trust is a large acute hospital Trust in the south east of England. We are an NHS provider organisation that provides a full range of general hospital services, and some areas of specialist complex care to around 560,000 people living in the south of West Kent and the north of East Sussex.

Our core catchment areas are Maidstone and Tunbridge Wells and their surrounding boroughs, and we operate from three main clinical sites: Maidstone Hospital, Tunbridge Wells Hospital and Crowborough Birth Centre. We employ over 5000 staff. We also provide specialist cancer services to around 1.8 million people across Kent, Hastings and Rother, via the Kent Oncology Centre, which is sited at Maidstone Hospital and at Kent and Canterbury Hospital in Canterbury. We also provide outpatient clinics in a range of locations in Kent and East Sussex.

Our Headquarters are located at Maidstone Hospital, Hermitage Lane, Maidstone Kent ME16 9QQ, and our main telephone number is 01622 729000.

We are registered as a Data Controller on the Data protection register of the Information Commissioner's Office (our registration number is Z9042352).

## 2. Your personal data

When you receive care and/or treatment from us, your illness and any treatment given is recorded (on paper records and/or on IT systems) to help us care for you.

This information is called "personal data" because it relates to you as an individual who can be identified. The ways in which we use your personal data are governed by law. The principal legislation that applies is the European Union's General Data Protection Regulation (GDPR) and the UK's Data Protection Act 2018 (DPA). In addition, confidential information that you give to our staff to enable them to provide your care and treatment is governed by the common law duty of confidentiality<sup>1</sup>.

When we use your information, the law calls this "processing". The personal data we process includes:

- Your name, date of birth, address, landline phone number, mobile telephone number and email address (if you have told us this)
- Whether you have a disability, allergies or health conditions
- Your next of kin and their contact details
- Details of contacts you have had with us, such as attendances at our Emergency Departments (EDs), inpatient stays, outpatient appointments and home visits
- Records and reports about your health and any treatment, care or support you need and receive
- Results of examinations and/or tests you have undergone and any associated diagnosis
- Details of your medicines, side effects and allergies
- Feedback on treatment outcomes
- Information from other professionals involved in your care and your family
- "Special category personal data", such as your race, ethnic origin, sex life and/or sexual orientation, religion or beliefs (see section 4 for further information)

---

<sup>1</sup> A duty of confidence arises when one person discloses information to another (for example a patient to a healthcare professional) in circumstances where it is reasonable to expect that the information will be held in confidence. This is a legal obligation derived from case law (i.e. rather than being an explicit requirement of any particular legal Act), and the obligation for information to remain confidential remains in place after a patient has died.

### **3. How we obtain and use your personal data**

#### **3.1 Obtaining your personal data**

The personal data we hold about you will either be provided directly by yourself (e.g. if you attend the Trust's EDs as a walk-in patient or answer questions asked by our healthcare staff), or by healthcare staff from other organisations. These include your GP, ambulance staff, other NHS provider organisations, Social Services and Independent Sector (i.e. private) healthcare providers.

We need accurate, up-to-date data about you because this:

- helps our staff assess your health and provide you with the right care and treatment;
- will help your future treatment, in hospital or elsewhere;
- allows us to review, and if necessary, look into the care and treatment you have received to determine whether this could have been better
- helps us provide high quality care and meet all our patients' needs;
- helps us train healthcare professionals and support research and development;
- helps us review (audit) the quality and outcome of NHS services;
- helps us investigate any incidents, complaints, concerns or issues that may arise;
- is necessary for the Trust to be paid for your treatment;
- contributes to national NHS statistics (which in turn helps the NHS plan its future services)

#### **3.2 Sharing your personal data**

We will share information about you with staff in other organisations when it is necessary for your care and treatment. These include your GP practice, other NHS providers involved in your care, ambulance services, Social Services and care homes.

The Trust is one of the partner organisations to the Kent and Medway Care Record (KMCR). The KMCR is an electronic care record which links your health and social care information held in different provider systems, to one platform. This allows health and social care professionals who have signed up to the KMCR to access the most up to date information to ensure you receive the best possible care and support by those supporting you. In order to enable this sharing of information, organisations who use the KMCR have agreements in place that allow the sharing of personal and special category data.

For further information about the Kent and Medway Care Record and the ways in which your data is used for this system please click [here](#).

Sometimes we have to pass on personal information by law, for example:

- to notify a birth;
- when an infectious disease such as meningitis or measles may endanger the safety of others;
- when required to by a formal court order;
- when sharing information with the Police may prevent a serious crime, or prevent harm to you or other people.

The law also requires us to share summary data about every episode of care with NHS Digital. You can find out how they use this information at: [NHS Digital: How we look after your health and care information](#).

We may also share information about you and your care with other NHS organisations responsible for the organisation and funding of health and social care, for example Clinical Commissioning Groups (CCGs) and their Commissioning Support Units (CSUs). If we have to share information about you, we will remove your personal details when possible (so that you are not able to be identified from such data).

### **3.3 Your choice for data to be used for research and planning purposes and the national data opt-out**

We may also use your personal data to assess how well our services are providing care, to suggest improvements and ensure that it is as good as it can be.

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

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

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

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

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

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

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

### **3.4 Patient Portal**

It is possible for you to access some of our services using NHS Login, a service created by the NHS for patients and the public to securely access their health and care information. NHS Login enables individuals to prove who they are safely and securely. The identity verification services are managed by NHS Digital. NHS Digital is the data controller for any information you provide to them to get an NHS Login account. To see NHS Digital's Privacy Notice and Terms and Conditions please see <https://access.login.nhs.uk/terms-and-conditions>.

### **3.5 More information**

You can also read more about why your data matters to the NHS, how it is protected and the choices you have on the national NHS website <https://your-nhs-data-matters>.

## **4. The legal basis for processing your personal data and your associated rights**

The GDPR includes 8 separate rights for individuals. However, the GDPR also obliges us to decide the specific legal basis under which we will process your personal data, and the rights you have are directly linked to the legal basis we rely on. Not all of the 8 rights apply to all legal bases.

#### 4.1 Direct clinical care and treatment

When your personal data is used for your direct clinical care and treatment, and the administrative purposes related to that care and treatment, including but not limited to the sending of appointments and associated reminders and surveys regarding the quality of care, we process that personal data on the basis of Article 6(1)e of the GDPR, which relates to that processing being necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Trust. The UK's Information Commissioner's Office (ICO) calls this legal basis "Public task", and the ICO expects most NHS provider organisations to rely on this legal basis for most of the data processing they do. This is because our underlying tasks, functions and powers have a clear basis in law (under numerous Acts of Parliament such as the Health and Social Care Act 2012).

**As we rely on the "Public task" legal basis when providing direct clinical care and treatment, only 6 of the 8 rights under the GDPR apply:**

- **The right to be informed.** This means that we must provide you with information about why we process your personal data, how long we hold that data, and who we share that data with. The ICO calls this "privacy information", and the Trust meets its obligations under this right through this Privacy Notice, which has been developed to comply with the ICO's expectations
- **The right of access.** You have the right to access the personal data that we hold about you. This is commonly referred to as "subject access", and asking to see your personal data is called a "Subject Access Request". Details of how to make a Subject Access Request can be accessed [here](#). The GDPR obliges us to respond to such requests within 1 month, and in most circumstances, we cannot charge a fee to deal with such requests.
- **The right to rectification.** You have the right to have inaccurate personal data rectified, or completed if it is incomplete. The DPA states that personal data is "inaccurate" if it is incorrect or misleading as to any matter of fact. If, for example, you therefore ask us to rectify a recorded opinion from a member of staff, we may not conclude that the record of that opinion is inaccurate and needs to be rectified, as opinions are, by their very nature, subjective. The GDPR obliges us to respond to such requests within 1 month. However, we can refuse a request for rectification if the request is manifestly unfounded or excessive (including taking into account whether the request is repetitive). There may also be some other exemptions under the GDPR or DPA that we judge should apply, but these exemptions will only be applied on a case by case basis. If you wish to request that your personal data be rectified, you should, in the first instance, discuss your request with the healthcare professional who is leading your care or treatment (this would usually be a Consultant medic). If you are not satisfied with the response, you can however contact the Trust's Data Protection Officer (please see section 6 for their contact details), and specify what data you believe should be rectified and why.
- **The right to restrict processing.** Restricting data processing means that we can store your personal data but not use it. You have the right to request that we restrict or suppress your personal data if:
  - You believe your personal data is inaccurate and you wish to verify the accuracy of that data;
  - You believe your personal data has been unlawfully processed (i.e. that we have breached the first principle of the GDPR<sup>2</sup>)
  - We no longer need your personal data but you need us to keep it in order to establish, exercise or defend a legal claim; or

---

<sup>2</sup> That personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject

- You have objected to us processing your data under Article 21(1) of the GDPR (the right to object – see below), and we are considering whether our legitimate grounds override your legitimate grounds

The GDPR obliges us to respond to requests to restrict processing within 1 month. If you wish to request that your personal data be restricted, you should contact the Trust's Data Protection Officer (please see section 6 for their contact details) and specify what data you believe should be restricted and why (making reference to one of the 4 reasons listed above).

- **The right to object.** As the Trust relies on the "Public task" legal basis, you have the right to ask us to stop processing your personal data. However, you must give specific reasons why you are objecting to us processing your data, and these reasons should be based upon your particular situation. You should also note that this is not an absolute right, and we can continue processing if we can demonstrate compelling legitimate grounds for the processing, which override your interests, rights and freedoms. If you wish to object to us processing your personal data, you should contact the Trust's Data Protection Officer (please see below for their contact details), and specify what data processing you are objecting to and why. However, if we are satisfied that we do not need to stop processing your personal data, we will let you know, and explain our decision. In such circumstances, you have the right to make a complaint to the ICO (please see below for their contact details) and/or seek to enforce your right through a judicial remedy (i.e. through the law courts).
- **Rights in relation to automated decision making and profiling.** Automated individual decision-making is when a decision is made solely by automated means without any human involvement. Profiling is the automated processing of personal data to evaluate certain things about an individual. Profiling can be part of an automated decision-making process. The GDPR has additional rules to protect individuals if they are subject to automated decision making and profiling. However, we do not process your personal data in this way, so those rules, and the associated rights, do not apply.

**You do not therefore have:**

- The right to erasure i.e. you do not have the right to have the personal data we hold about you erased. You do however have a right to restrict how we process that data (please see above);
- or
- The right to data portability i.e. you do not have the right to obtain and reuse the personal data we hold about you for your own purposes across different services, nor to ask that we copy or transfer the personal data we hold in our IT environment to another such environment in a safe and secure way, without affecting its usability.

#### **4.2 Secondary (i.e. indirect) care purposes**

When your personal data is used for secondary (i.e. indirect) care purposes, we process that personal data on the basis of Article 6(1)c of the GDPR, which relates to that processing being necessary for compliance with a legal obligation to which we are subject. This applies to when there is a legal requirement for us to provide specified data to, for example, organisations such as NHS Digital. In cases where the common duty of confidentiality<sup>3</sup> cannot be satisfied through consent we seek approval from the Secretary of State for Health and Social Care via the Confidentiality Advisory Group under Section 251 of the National Health Service Act 2006.

---

<sup>3</sup> A duty of confidence arises when one person discloses information to another (for example a patient to a healthcare professional) in circumstances where it is reasonable to expect that the information will be held in confidence. This is a legal obligation derived from case law (i.e. rather than being an explicit requirement of any particular legal Act), and the obligation for information to remain confidential remains in place after a patient has died.

**As we rely on the “Legal obligation” legal basis when processing your personal data for secondary (i.e. indirect) care and treatment, only 5 of the 8 rights under the GDPR apply** (please see section 3.1 above for further details of these rights):

- The right to be informed
- The right of access
- The right to rectification
- The right to restrict processing
- Rights in relation to automated decision making and profiling

**You do *not* therefore have the following rights** (see section 3.1 above for further details of these rights):

- The right to erasure
- The right to data portability
- The right to object

#### **4.3 Research**

We may share data for approved research projects. In most instances the information will be made anonymous so that you cannot be identified.

If this is not possible, we will process your personal data on the basis of Article 6 (a) of the GDPR, which relates to you giving consent to that processing.

Where it has been impracticable to obtain your consent we will seek approval from the Secretary of State via the Confidentiality Advisory Group under Section 251 of the National Health Service Act 2006.

### **5. The legal basis for processing special categories of personal data**

Special category data is personal data which is more sensitive, and so needs more protection (as this type of data could create more significant risks to a person’s fundamental rights and freedoms, by putting them at risk of unlawful discrimination). Such data includes information about an individual’s race; ethnic origin; politics; religion; trade union membership; genetics; biometrics (where used for ID purposes); health; sex life; or sexual orientation. The GDPR obliges organisations that process special category data to decide the additional, specific, legal basis under which we will do this.

It is important for us to have a complete picture, as this information helps staff involved in your care to give personalised care, deliver appropriate treatment and care plans and meet your needs. We therefore process special category data relating to your health, and we may process data relating to your race, ethnic origin, sex life and/or sexual orientation. We process such data on the basis of condition h of Article 9(2) of the GDPR, which relates to such processing being necessary for the provision of health or social care or treatment or the management of health or social care systems and services on the basis of European Union or UK law.

### **6. Our Data Protection Officer (DPO)**

As we are a public authority, the GDPR requires us to appoint a Data Protection Officer (DPO), and our Trust Secretary has been appointed to that role. Our DPO assists us to monitor internal compliance with the GDPR, informs and advise us on our data protection obligations, provides advice regarding Data Protection Impact Assessments (DPIAs) and acts as a contact point for data subjects and the ICO.

Our Data Protection Officer can be contacted via email ([kevinrowan@nhs.net](mailto:kevinrowan@nhs.net)) or telephone (01622 228 698).

## **7. Retention periods**

We hold personal data for specified periods of time, as set out in the [Records Management Code of Practice for Health and Social Care 2016](#).

## **8. Transfers of personal data to data controllers and processors located outside the European Economic Area (i.e. third countries) or international organisations**

We do not transfer any of your personal data to data controllers and processors located outside the European Economic Area (i.e. third countries) or international organisations

## **9. Your right to complain**

If you wish to complain about how we have processed for personal data, you should, in the first instance, contact our complaints team, describe the nature of your complaint, and (ideally) state what action you would like the Trust to take.

Our Complaints Department can be contacted by email at [mtw-tr.complaints@nhs.net](mailto:mtw-tr.complaints@nhs.net) or via:

The Complaints Department  
Maidstone and Tunbridge Wells NHS Trust  
Maidstone Hospital  
Hermitage Lane  
Maidstone  
Kent ME16 9QQ

If you are dissatisfied with the outcome, you have the right to ask the Information Commissioner's Office (ICO) to investigate your complaint, using the ICO's website, at <https://ico.org.uk/make-a-complaint/your-personal-information-concerns/>.