



# Manchester University

NHS Foundation Trust

## PRIVACY INFORMATION

### YOUR RIGHT TO BE INFORMED

#### How we use your personal information

- **Why we collect information about you**
- **How personal data about you is used**
- **Your rights**
- **How we keep personal data about you confidential**

## **Manchester University NHS Foundation Trust (MFT)**

Manchester University NHS Foundation Trust (MFT) is a major NHS Trust providing services for adults and children across Greater Manchester and beyond. As well as providing general and specialist health care, it plays an important role in the teaching and education of health care professionals and in healthcare research and innovation.

We have ten hospitals; Altrincham Hospital, Manchester Royal Eye Hospital, Manchester Royal Infirmary, North Manchester General Hospital, Royal Manchester Children's Hospital, Saint Mary's Hospital, Trafford General Hospital, University Dental Hospital of Manchester, Wythenshawe Hospital and Withington Hospital. We provide services to our community through the Manchester Local Care Organisation and Trafford Local Care Organisation and host a small number of organisations such as Health Innovation Manchester.

MFT is the Data Controller for the information it collects and records, uses and stores about its patients, carers, staff and the public. MFT processes its data electronically and using paper-based systems.

This is our Privacy / Transparency Notice which informs you how and why we process your personal data.

## Legal notification

We are registered with the Information Commissioner's Office (ICO).

Our registration number is ZA282424

If you would like to look at our registration, please go to the Data Protection register on the ICO website or use the link:

<https://ico.org.uk/esdwebpages/search>

We process personal data under the Data Protection Act 2018 (DPA 2018) and the UK General Data Protection Regulation (UK GDPR). During the Covid-19 pandemic we processed some health data under the Health Service (Control of Patient Information) Regulations 2002.

## Lawful Basis for Processing

We will only process information relating to you as long as there is a lawful basis as described in the DPA 2018 and the UK GDPR and it is necessary to do so. We may use one of the following lawful bases:

- Public Task – this is the lawful basis that we will mostly use to deliver our services as an NHS organisation
- Legitimate interest – where we need to process your data for the day to day running of our Trust other than for the performance of our public task
- Vital interest – when it is necessary to protect someone's life
- Legal obligation – where we need to comply with the law
- Contract – in order to perform our contract with you

Where none of these are appropriate, we will then approach you for your consent.

# **PATIENTS AND CARERS**

## **What we collect and record about our patients and carers**

We keep records about your health, treatment and care which is mostly held electronically, however occasionally the data may be held in paper format. Details of the information we keep include, but are not limited to:

- personal details such as your name, address, date of birth, telephone numbers, email address, ethnicity and religion, NHS number and your next of kin.
- contact we have with you e.g. hospital admissions, outpatients/clinic appointments and home visits.
- notes and reports made by health and care professionals about your health, GP details etc.
- details and records about your diagnosis, treatment and care.
- results of x-rays, laboratory tests, and any other health related tests
- drug prescriptions, clinical photography
- relevant information about people that care for you and know you well.
- basic details about associated people e.g. your spouse / partner, children, carers, relatives etc.

This information may be given to us directly by you. 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.

Our hospitals use our electronic patient record (EPR), known as EPIC Hive. We also have other clinical systems which are used by specialist services including EMiS which is used by our community staff; and PARIS which is used by our Child and Adolescent Mental Health Services (CAMHS).

Our EPR system EPIC Hive has a patient portal known as MyMFT, which allows you to have fast, secure access to your health information held by the Trust. It will also allow you to review and update personal details that we hold for you such as your home address, mobile phone number and email address.

Details on how to sign up to the MyMFT patient portal including downloading the app can be found on the MFT website, link: <https://mft.nhs.uk/the-trust/mymft/>

Proxy access to your record may also be granted for family members and carers to help you manage your care. Please note, this is not automatic and requires an authorisation process. Details on Proxy access can be found on our website using the above link.

Our staff document and use information about you as part of our provision of health care to you. The staff who do this include doctors, nurses, administrative & support staff and other health & care professionals.

We may also hold information relating to your direct care which has been provided to us by other NHS organisations such as your GP, other NHS hospitals, NHS clinics, and other third parties such as Opticians, Dentists, Pharmacists, private healthcare providers, or from other bodies such as university and schools.

## **Processing your data for direct care, education/training, administrative purposes, clinical trials and research**

We need to collect, record, store and use your personal data in order to provide our healthcare services to you. The Trust has a lawful basis for processing personal data and meets the DPA 2018 and UK GDPR condition for processing special category data, which includes (but is not limited to) racial or ethnic origin, genetic data, health data and sexual orientation. As an NHS organisation, most of our processing is undertaken using the lawful basis of public task; this is the exercise of our official authority or in the public interest of health care provision including research, education and teaching and is under the legal governance of the DPA 2018, the UK GDPR, the NHS Plan 2000, the Health Services Act 2006, Health & Social Care Act 2012 and the Care Act 2015.

### **How is your information used?**

Your information is used for direct care, education/teaching, administrative purposes, health research and innovation which may include (but is not limited to):

- providing you with care and treatment, both now and in the future.
- ensuring that appropriate information is available to all those who treat you medically and care for you professionally
- sharing information with staff employed by MFT and also with other NHS and Non-NHS organisations that may provide care for you
- supporting you in managing your own care
- helping our staff review (audit) the care they provide to you to ensure it is of the highest standard, safe and effective

- training and teaching our healthcare professionals so that they can experience, learn and train with real health care scenarios
- research & innovation to develop and improve the provision of healthcare

As part of The NHS Constitution, the NHS commits “to ensure those involved in your care and treatment have access to your health information so they can care for you safely and effectively (pledge)”. To assist with this commitment, the Trust routinely sends your GP a letter detailing the outcome of any episode of care that you have received whilst under our care.

We will also share proportionate information about your direct care with other NHS and Non-NHS organisations to help them provide direct care for you.

Your health record is critical to providing the best care for you and we may automatically share this data through secure electronic systems, such as the Greater Manchester Care Record (GMCR), other organisations using EPIC EPR, and other patient systems used by our partners in local health care and social care settings, including the community Local Care organisations and the independent sector.

In some of these cases, we become a Joint Data Controller with the other organisations when we use the same systems.

We make sure that we have agreements in place with these organisations so that each organisation is aware of its data protection responsibilities and that your personal data is kept secure and confidential, used for the purpose for which it was provided and is only accessed when there is a lawful basis to do so.

## **We may also use your information for other purposes such as to:**

- properly investigate any complaint, incident report or legal claim about your care that may be made by you or someone on your behalf
- look after the health of the general public
- manage and plan the health services we provide to you
- send local and national surveys relating to the services you use

On occasion, we may need to share information about you to organisations that do not provide direct care but provide additional support for your health and wellbeing or to support public health such as during an epidemic or pandemic.

The information we share always meets Data Protection legislation and follows NHS Caldicott principles to ensure that it is relevant and proportionate for the purpose for which it is being used. Examples of other organisations that we share information with include, but not limited to:

- Education services, for example, schools
- Voluntary service providers
- Sure Start teams
- The Police, Fire and Ambulance Services
- Government departments
- Housing departments

We may also share your information where we have a legal obligation, for example where:

- we receive a formal court order
- there is a need to protect and safeguard vulnerable children and adults



- there is a public health need such as during a pandemic, or if you have an infectious disease
- there is a statutory power

The above are only some examples and are not exhaustive.

We may also use your data to provide:

- anonymised information - where your data is rendered into a form which does not identify you. This data cannot be converted back into identifiable format.

or

- pseudonymised information - where your identifying data is replaced with non-identifiable data so that your 'real world' identity is removed and the data shared is not identifiable to the recipients of the data. This data can only be converted back into identifiable format by an authorised, restricted key-holder and in most cases the key-holder is only ourselves.

Sharing anonymised and pseudonymised data is done through a strict approval process to ensure it is safe and secure and only used for the purpose for which it is being provided.

## **Your mobile phone number**

We hold your mobile telephone number to enable us to contact you if an appointment has to be rearranged, or to give you important information about your health, for example if you have been in contact with an individual who may have passed an infection to you or if you need urgent healthcare.

Some services also provide a text reminder service to keep you updated about your appointment and to send you reminders. If you prefer not to be contacted in this way, please tell us so we

can make a note of this on your record. You can also set your communication preferences through the MyMFT Portal.

## **Your Email Address**

We hold your email address so that there is an alternative way to contact you.

When our staff send you an email then we will encrypt the email correspondence if it contains sensitive health data unless you specifically ask us not to.

If you send us an email regarding your health care, including details of diagnosis or treatment, we will generally respond back to you using email which is without encryption. Emails via MyMFT portal are also not encrypted.

Once we have sent you an email, we are not able to maintain the security and confidentiality of that email or its attachments. You are responsible for emails that have been sent to the email address you provided to us.

## **Health Research and Innovation**

As part of our official authority as an NHS Trust we undertake important health and care research and innovation. We use the lawful basis of Public Task for processing data for research purposes and innovation.

All research conducted at the Trust is approved by the Health Research Authority (HRA) who assess that it is compliant with UK law and regulations, including where required, an NHS Research Ethics Committee review. Research initiated and sponsored by the Trust is assessed to ensure it meets current regulations.

The patient data and research published by the HRA can be accessed through the link below:

<https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-guidance/templates/template-wording-for-generic-information-document/>

## **The National Data Opt-Out Programme**

Information about your health and care helps us to improve your individual care, speed up diagnosis, plan your local services and research new treatments.

The national data opt-out is a service that allows you to opt-out of your confidential patient information being used for research and planning.

You do not need to do anything if you are happy about how your confidential patient information is used.

If you do not want your confidential patient information to be used for research and planning, you can choose to opt-out securely online or through a telephone service

To find out more or to make your choice, visit

<https://www.nhs.uk/your-nhs-data-matters>

or call 0300 303 5678

## **OTHER PROCESSING**

As well as processing for health care we undertake other data processing as part of our business. The lawful bases that are mostly used in our other processing are contract, legal obligation and legitimate interest.

### **Employment Data**

We keep personal and special category data about:

- staff who are currently or have previously been employed by us
- prospective staff applying for jobs with us
- volunteers, casual (bank) staff, contractors, agency workers
- staff working for our hosted organisations

We hold employment information which is processed, for specific purposes, such as administration, management and operation of your employment, occupational health and wellbeing, or in relation to the Trust's legal obligations or organisational needs. This applies to data held on computer or on paper.

Information we hold about our staff includes but is not limited to name, address, date of birth, gender, ethnicity, religion, disability information, next of kin, emergency contact details, job application details (CVs), recruitment and employment checks including proof of identification and right to work in the UK, employment references, employment details, national insurance number, bank details, pension details, Disclosure and Barring Service checks, appraisals, employee relations information including investigations and outcomes, trade union membership, employee health and wellbeing information, absence data, data relating to accidents

and injury at work, Professional registrations, training relating to your employment.

We also hold your car registration number(s) to manage any car parking permit that you have.

We may share information about our staff with third parties where we are required to by law, for example with His Majesty's Revenue and Customs (HMRC), Department of Work & Pensions, National Fraud initiatives / prevention and detection of crime, independent mandatory public authority reviews. We also share information as part of our contract with you for example with NHS Business Services Authority for maintaining your employment and pension records held on the national NHS Electronic Staff Record (ESR); or where we or a third party has a legitimate interest, for example to manage our carparks.

## **Trust Governors and Trust Members**

If you are a Trust Governor or a Trust member, we hold information about you which is processed for specific purposes associated with being a Trust Governor and / or Foundation Trust Member. Information we hold include personal information such as your name, date of birth, correspondence address. We use your personal data in order for us to communicate to you about the Trust and its activities.

The Department of Health ask us to collect your ethnicity, language and disability status so that we can be sure that we are representing all sections of our communities.

## **CCTV (closed circuit television), Body Cameras, ANPR**

We use CCTV in some parts of our hospitals and grounds to help us maintain the safety and security of individuals and property; and for prevention and detection of crime, to facilitate the apprehension and prosecution of offenders and apprehension of suspected offenders; or as necessary in the public interest such as preventing or detecting unlawful acts or protecting the public against dishonesty.

CCTV is used under strict guidelines and in line with national legislation and guidance.

We use automatic number plate recognition (ANPR) so that we can manage our car parking securely and effectively.

Some staff wear body cameras and these are only used in exceptional circumstances in line with national guidance.

We process data captured by CCTV, ANPR and body cameras as part of our legitimate interests. The data is automatically deleted after 30 days unless we have a lawful basis to retain it for longer.

## **Our Charities**

We collect your personal information when you ask about our activities, to donate, register to receive our newsletters or otherwise give us personal information. We use this information to help us process donations, newsletter requests and enquiries. We may also use this information to help us understand your needs and provide you with a better service.

We use the lawful basis of legitimate interest to process your data.

We will ask for your consent when we want to send electronic marketing to you for the first time. You will be able to opt-out at any time, either via an opt-out option on the email or by contacting us.

## **Our Nursery**

If you use our nursery, we collect information about you and your child when you register for our nursery. The information we hold about your child includes name, date of birth, ethnicity, religion, health information such as medication, allergies, dietary requirements, photographs, GP and health visitor information, and base-line assessment.

We hold your name and contact information and name and contact details of persons authorised to collect your child. We also hold your chosen fee payment details so that we can process nursery fees.

We use your child's details to assess, support and track your child's learning, activities, assessments, trends, development, recording accidents, manage medicines and other special needs and comply with Early Years and Ofsted requirements.

We share your child's data where required, with your Child's Health Visitor, School Teacher, Quality Assurance Framework Team.

## INDIVIDUAL RIGHTS

### Accessing your information (Right of Access)

You have the right of access to the personal data we hold about you. This is sometimes referred to as a Subject Access Request (SAR). To help us process your request we will require you to provide proof of your identity and some clarity about the information you require.

A form is available to help with the request.

For our patients and carers, the form can be accessed on our external website ([www.mft.nhs.uk](http://www.mft.nhs.uk)) or it can be provided by contacting the Subject Access Health Records (SAHR) team:

by email: [sar.mft@mft.nhs.uk](mailto:sar.mft@mft.nhs.uk)

by telephone: 0161 701 1303 / 1315

by post: SAHR Team, Manchester University NHS Foundation Trust, Manchester Royal Infirmary, Oxford Road, Manchester M13 9WL

**Staff:** If you are a member of staff then you should contact your line manager in the first instance.

### Other Rights:

In addition to the Right to be Informed (i.e. this privacy notice) and the Right of Access, which is documented above, you also have the:

- Right to Rectification
- Right to Erasure (Right to be forgotten)\*



- Right to Object
- Right to Restrict Processing
- Right to Data Portability
- Right not to be subject to automated decision making including profiling

\*The right to erasure and right to data portability are not applicable when processing on the lawful basis of a public task.

If you would like to exercise any of these rights, please contact:

The Data Protection Officer

Manchester University NHS Foundation Trust (MFT)

Group Digital

Cobbett House

Oxford Road

Manchester

M13 9WL

Telephone 0161 701 0375

Email: [dpo@mft.nhs.uk](mailto:dpo@mft.nhs.uk)

We will consider your request and respond to you within a calendar month.

## KEEPING YOUR DATA SECURE AND CONFIDENTIAL

We keep all paper and electronic records securely, to ensure confidentiality, integrity and availability and prevent unauthorised access.

The sensitivity of patient information is well understood within the NHS. Our staff are required to undertake annual training on their data protection and confidentiality responsibilities and these responsibilities are written into employee's contracts.

Our Contractors, Agency Staff and Volunteers have confidentiality clauses in their contracts and we have Data Processor contracts with those Suppliers who carry our data processing activities for us.

MFT staff have their own unique logon credentials (username / password or Smartcard) for accessing Trust systems; and can only access those Trust systems necessary for their job role. Within each individual system, their access is also in line with the individual's job role. This ensures confidential data is on a "need to know" basis.

We will undertake a Data Protection Impact Assessment (DPIA) where necessary, for example at the start of any major new project that involves the use of personal data or introduces new technologies.

We do not sell any personal data we hold.

We do not routinely transfer any information to countries outside the UK. If your information is to be sent outside of the UK we will undertake a DPIA to ensure transfer is in accordance with Data Protection legislation and any identified risk is mitigated.

We use cookies which are harmless text files on all our websites. These are to improve your browsing experience and enable certain features or functionality.

We do not use cookies for advertising purposes or pass associated data derived from the cookies to any other organisation. Further information on the use of cookies can be found on our websites.

In the event of a data breach, this will be logged on our Incident Reporting system and fully investigated, with remedial action taken where required. We will report certain types of personal data breach to the Information Commissioner's Office (ICO).

On an annual basis, we complete the NHS Data Security and Protection Toolkit which demonstrates our compliance against the NHS National Data Guardian's ten Data Security Standards.

## **Retention of data**

We keep your data for as long as required in line with national NHS England Records Management Code of Practice; A guide to the management of health and care records. It covers paper and digital records and includes guidance on patient records, staff records, complaint records and corporate records.

For further information please use "NHS records management code of practice" in an internet search engine.

## The Information Commissioner's Office

If you would like independent advice about data protection or if you are not satisfied with the handling of your rights under data protection, you can contact:

The Information Commissioner's Office

Wycliffe House

Water Lane

Wilmslow

Cheshire

SK9 5AF

Tel: 0303 123 1113

Website: [www.ico.org.uk](http://www.ico.org.uk)