

This Privacy Notice tells you about information we collect and hold about you, what we do with it, how we will look after it and who we might share it with.

It covers information we collect directly from you or receive from other individuals or organisations. The law strictly controls the sharing of some types of personal information and the Trust ensures full compliance with the Data Protection Act 2018 when processing its data. However within the law, the information about you may be passed onto others for your continuing healthcare and treatment.

This notice is not exhaustive. However, we are happy to provide any additional information or an explanation if needed. To contact us about any of the points in this notice please see the contact details at the end of this notice.

Our Commitment to your Data Privacy and Confidentiality



We are committed to protecting your privacy and will only process **personal confidential data** lawfully and in accordance with the Data Protection Act 2018. Incorporating the General Data Protection Regulations (GDPR), the Privacy and Electronic Communications Regulations (PECR), the Common Law Duty of Confidentiality and the Human Rights Act 1998.

MKUH is a Data Controller under the terms of the Data Protection Act. We are legally responsible for ensuring that all personal information we hold and use is done so in compliance with the law. All data controllers must ensure they are compliant of the Data Protection Act 1998. More information can be found on the [Information Commissioner's website](#).

Everyone working for the NHS has a legal duty to keep information about you confidential. The NHS Care Record Guarantee, the NHS Constitution, the Health and Social Care Information Centre Guide to Confidentiality as well as the NHS Confidentiality Code of Practice provide a commitment that all NHS organisations, and those providing care on behalf of the NHS will use records about you in ways that respect your rights and promote your health and well-being. What is this page about?

We will not share information that identifies you unless we have a fair and lawful basis on which to do so:

- To ensure your safe care and treatment
- To protect children and vulnerable adults
- When a formal court order has been served on us
- When we are lawfully required to report certain information to the appropriate authorities
- To protect the health and safety of others e.g. Emergency Planning reasons
- When permission is given by the Secretary of State for Health or the Health Research Authority (HRA) on the advice of the Confidentiality Advisory Group to process confidential information without the explicit consent of individuals.

If you are receiving services from the NHS, we share information that does not identify you (anonymised) with other NHS and social care partner agencies. This is done for the purpose of improving local services, research, audit and public health. This is an important part of our processing as it ensures that the NHS keeps improving its standards and treatments.

We also anonymise information for Indirect Care so that we can:

- Review our planning and services so that we meet patients expectations and needs
- Prepare statistics and performance figures
- Safeguard the health of the general public
- To provide training and continuing education for our staff.

Personal Data we hold about you

Your information is held by the Trust so we can ensure we give you the correct care and treatment.

There are many definitions of personal data, please see below which may be of use to you.

Personal Data

This refers to any information relating to an identified living individual.

- Directly or indirectly, in particular, by reference to an identifier such as a name
- An identification number
- Location data
- An online identifier e.g. including IP address and internet cookies

- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person

Special Categories

This is defined in the Data Protection Act as information about an identifiable factor.

- Racial and ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union Membership
- The processing of genetic data
- Biometric data for uniquely identifying an individual
- Data concerning health
- Data concerning an individual's sex life or sexual orientation

Processing Personal Data

This means any operation or set of operations which are undertaken on personal data, whether by automated means or not.

- Collection, recording, organisation, structuring Or storage
- Retrieval, consultation or use
- adaptation or alteration
- disclosure by transmission, dissemination or making available
- alignment or combination
- restriction, erasure or destruction

Personal Confidential Data

This is personal information about identified or identifiable individuals which is also confidential. 'Personal' includes the Data Protection Act definition of personal data, but is also includes the deceased as well as the living. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' e.g. health records. It is adapted to include 'special categories' data as defined in the Data Protection Act.

Pseudonymised Information

This means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific individual without the use of additional information, provided that information is kept separately.

Anonymised Information – this is data that has been changed into a form which does not identify individuals or where there is little risk of identification.

Aggregated Information

This is anonymised data that is grouped together so that it does not identify any individuals.

Retention Schedules

The Trust ensures that information is not kept for any longer than is necessary in line with the Data Protection Act 2018 – incorporating GDPR. The Trust abides by the [NHS Retention Schedules](#).

Access to Health Records

The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information.

What are you entitled to?

- confirmation that we are processing your personal data
- a copy of your personal data
- other supplementary information (this is covered in our Privacy Policy)

You are only entitled to your own personal data, and not to information relating to other people (unless the information is also about you or you are acting on behalf of someone).

Accessing your own health information

To gain access to your own health records, complete the [Access to health records form](#).

Accessing your child's health record

For health records that belong to a child please complete the [Access to child's health records form](#).

Please note that if the child is 13 years of age or over, we may ask to see proof of their consent.

Accessing a patient's health information as a nominee

To make a request for health records of a patient as a nominee, you will need to complete the [On Behalf of Patient Record Form](#).

Accessing a deceased patient's health record

The Access to Health Records Act 1990 gives deceased patient's personal representation and anyone who may have a claim arising out of the patient's death,

a right of access to the patient's clinical records. This is not a general right and access may be limited to information of relevance to the possible claim.

Access can be limited or refused if:

- there is evidence the patient would not have expected the information would be disclosed to the applicant
- if the disclosure is likely to cause serious harm to anyone else
- if it would also disclose information about a third party who does not consent
- the records contain a note, made at the patient's request, that they did not wish access to be given on an application under this legislation

To make a request for any deceased patient's health record we may hold you will need to complete the [Deceased Patient Record Form](#).

Return the completed form to us attaching your proof of identity documentation.

email: accesstohealthrecords@mkuh.nhs.uk

post: Information Governance Department, Milton Keynes University Hospital, Standing Way, Eaglestone, MK6 5LD.

Fees

We will not charge a fee for providing your information, your child's health record, as a nominee for a patient or that of a deceased family member. However, we may charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. We may also charge a reasonable fee to comply with request for further copies of the same information. The fee will be based on the administrative cost of providing the information.

Viewing health records

An appointment **MUST** be arranged with the [Information Governance Department](#) prior to viewing records electronically. Please contact us on 01908 995 042. Viewing your health records is free of charge.

The Trust will endeavour to deal with your request within a 21 day time limit (NHS best practices). However, by law we have 30 days to respond. If this is likely to take longer the applicant will be warned and an explanation of the delay provided.

Health Insurance Claim Forms

We officially stamp your health insurance claim forms.

The Information Governance team are happy to stamp your claim forms between the hours of 07:30 - 16:30

We do NOT charge for this service.

Purposes for using your information

Milton Keynes University Hospital embraces transparency as a means of building trust and confidence with our patient/staff.

Being transparent and providing accessible information to individuals about how we will use personal data is a key element of the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR).

We want to be clear about the purpose/purposes for which we hold personal information and data.

It is often argued that people's expectations about personal data are changing. People are increasingly willing to share information on social media and to allow their data to be collected by mobile apps, but they are unwilling to read lengthy privacy notices.

These factors are sometimes used to support the view that they are relatively unconcerned that their data is being collected and processed. However, we believe that people do have concerns about how organisations handle their data and want to retain some control over its further use.

Therefore, we have separated our full privacy notice into easy to read sections as it is important for us to be transparent about our processing and comply with the legal requirements to provide privacy information.

- [Direct and indirect care](#)
- [Safeguarding](#)
- [Complaints](#)
- [Invoice validation and support services](#)
- [Clinical research](#)
- [Fundraising](#)
- [Patient experience and engagement](#)
- [Membership and Volunteers](#)
- [Staff Employment](#)

Your information will not be sent outside of the United Kingdom unless there is a clinical need to do so.

We will always ensure that your privacy is protected in the same way overseas as it is here in the UK. We will never sell any information about you.

Your Rights

You have a right to privacy and to expect the NHS to keep your information confidential and secure.

Under the Data Protection Act 2018 (DPA 2018) it becomes a legal right to ensure that your data is processed on a fair and lawful basis and in a transparent manner.

Right to be informed

The information we supply about the processing of personal data must be:

- concise
- transparent
- intelligible and easily accessible
- written in clear and plain language if addressed to a child
- free of charge

Right of access

You can find out if we hold any personal information by making a 'subject access request' under the DPA 2018. If we do hold information about you, we will:

- give you a description of it
- tell you why we are holding it
- tell you who it could be disclosed to
- let you have a copy of the information in an intelligible format

Right to rectification (correction)

You are entitled to have personal data rectified if it is inaccurate or incomplete. If we have disclosed the personal data in question to others, we must contact each recipient and inform them of the rectification – unless this proves impossible or involves disproportionate effort. If asked to, we must also inform you about these recipients.

We have one month to respond to a request for rectification. This can be extended by two months where the request for rectification is complex. If we decide not to take

action in response to a request for rectification, we will explain to you the reasons why and explain your right to complain to the supervisory authority.

Right to erasure (to be forgotten)

The right to erasure does not provide an absolute 'right to be forgotten'. You have a right to have personal data erased and to prevent processing in specific circumstances.

- where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed
- when you withdraw consent
- when you object to the processing and there is no overriding legitimate interest for continuing the processing.
- the personal data was unlawfully processed (i.e. otherwise in breach of the DPA 2018 and GDPR)
- the personal data has to be erased in order to comply with a legal obligation
- the personal data is processed in relation to the offer of information society services to a child

This right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

We can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information
- to comply with a legal obligation for the performance of a public interest task or exercise of official authority
- for public health purposes in the public interest e.g. archiving purposes in the public interest, scientific research, historical research or statistical purposes or the exercise or defence of legal claims

Please note that the right to be forgotten does not apply to special category data i.e. medical records.

Right to restrict processing

We will be required to restrict the processing of personal data in the following circumstances:

- where you contest the accuracy of the personal data, we should restrict the processing until the accuracy of the personal data has been verified
- where you have objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests) and we are considering whether we have legitimate grounds to override your rights
- when processing is unlawful and you oppose erasure and request restriction instead
- if we no longer need the personal data but you require the data to establish, exercise or defend a legal claim

We will continue to review procedures to ensure we are able to determine where we may be required to restrict the processing of personal data.

Right to data portability

The right to data portability allows you to obtain and reuse your personal data for your own purposes across different services.

It allows you to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The right to data portability only applies:

- to personal data you have provided to the Trust
- where the processing is based on your consent or for the performance of a contract and when processing is carried out by automated means

Right to object

You must have an objection on 'grounds relating to your particular situation' in order to exercise your right to object to processing for research purposes. If we are conducting research where the processing of personal data is necessary for the

performance of a public interest task, we are not required to comply with an objection to the processing.

We will stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no grounds to refuse.

You have the right to object to the following:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing (including profiling)
- processing for purposes of scientific/historical research and statistics

We will stop processing the personal data unless:

- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual
- the processing is for the establishment, exercise or defence of legal claims

We do not carry out profiling and/or automated decision-making. This is documented in our data protection policy.

Fees

We will not charge a fee for providing your information. However, we may charge a 'reasonable fee' when a request is manifestly unfounded or excessive, particularly if it is repetitive. We may also charge a reasonable fee to comply with request for further copies of the same information. The fee will be based on the administrative cost of providing the information.

The Trust will endeavour to deal with your request within a 21 day time limit (NHS best practice). However, by law we have 30 days to response, if this is likely to take longer, the applicant will be warned and an explanation of the delay provided.

For further information please contact the Information Governance Team

Data Protection Officer

Tel: 01908 995041

Email: dataprotectionofficer@mkuh.nhs.uk

Information Governance Team:

Tel: 01908 995045

Email: askig@mkuh.nhs.uk

Access to Health Co-ordinator

Tel: 01908 995042

Email: accesstohealthrecords@mkuh.nhs.uk