

PATIENT & PUBLIC PRIVACY NOTICE

APPENDIX A: PATIENT & PUBLIC PRIVACY NOTICE

When we process your personal data, Kettering General Hospitals Foundation Trust (KGH) is the Data Controller. As a Data Controller, the Trust has a duty to comply with the General Data Protection Regulation (GDPR), which requires that processing of your personal data is **fair, lawful**¹ and **transparent**. This means we must:

- Keep sufficient information to provide services and fulfil our legal responsibilities
- Keep your records secure and accurate
- Only keep your information as long as necessary
- Collect, store and use the information you provide in a manner that is compatible with the data protection legislation.

Furthermore, we have a legal obligation to respect the common law duty of confidentiality. All of our staff are contractually bound to this obligation through their terms and conditions of employment. Healthcare professionals are further committed to maintaining confidentiality through their professional registration.

The Trust is registered as a data controller with the Information Commissioner's Office – registration number Z4936855. Our registration entry can be seen [here](#).

Why do we need information about you?

In order to provide you with the highest quality of healthcare we need to keep records about you. Health records comprise information relating to your physical or mental health, created by a healthcare professional to support your care. Health records consist of electronically-held information, such as radiology images and test results, and include paper records which have been scanned. Records also include referral and discharge letters, observation charts, outpatient/inpatient clinical notes, and relevant information from people who care for you and know you well such as health professionals and relatives/carers.

How your personal information is used

The people who provide healthcare to you, such as your doctor, nurse or other healthcare professional will use your records to:

- Confirm who you are when we contact you, or when you contact us
- Make decisions about your ongoing care and treatment
- Make sure your care is safe and effective, for example, for clinical audits.

¹ General Data Protection Regulation

- Article 6. 1. (e) - processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller
- Article 9. 2. (h) - processing is necessary for the purpose of the provision of health or social care or treatment, or the management of health and social care systems

Who do you share my information with?

We recognise our duty to share information about our patients with healthcare professionals from other organisations to ensure safe and effective continuity of your care. We do so under a formal agreement about how it will be used and kept confidential. Some examples are:

- This Trust is part of a group of NHS hospitals in the East Midlands that have a shared NHS radiology system. This will enable healthcare professionals in other NHS hospitals in the East Midlands to access your radiology record when necessary, to ensure you receive consistent, safe and effective clinical care and treatment, irrespective of where you receive your care. For further information click [here](#)².
- The Trust is a member of the Northamptonshire Healthcare Partnership. The community portal enables providers to electronically share your health and social care information, such as hospital and GP attendances, test results, medication and care plans with other Northamptonshire health and social care providers. With your explicit consent, health and social care professionals, or staff who are supervised by health and social care professionals, will be able to access this information to better coordinate and provide care to you..
- When Children and Young People attend KGH information may be shared with relevant health care professionals e.g. Health Visitor, School Nurse
- We may also share relevant information about you with other NHS organisations such as:
 - Other hospitals and healthcare providers that are involved in your care and treatment
 - Your GP.
- If you are receiving care from other services outside the NHS, for example social care services, we may need to share information about you so we can all work together for your benefit. For example, we may share your information with:
 - Social Care Services
 - Local Authorities
 - Voluntary and private sector providers working with the NHS.

Do I have a choice?

If you wish to receive safe and appropriate care and treatment at our hospital we must maintain an accurate record of relevant information about you. If you have any concerns about providing information, or how we share it with other health and social care providers, please discuss this with our staff so that you fully understand the potential impact on your care or treatment.

Do you ever share my information without my consent?

We will not disclose your information to any other third parties for non-care purposes without your consent unless there are exceptional circumstances or where we are legally required to report information to the appropriate authorities. For example:

- Notifications of:

² See Appendix D

- new births
- diagnosis of infectious diseases such as meningitis or measles (but not HIV or AIDS) which may put other people at risk
- To comply with a court order
- Public interest, for example, if there is a risk of death or serious harm
- A legal need to share it, for example:
 - to protect a child under the Children Act and Local Safeguarding Procedures
 - to support investigations by the Counter Fraud Agency
- A legitimate enquiry from the police under data protection legislation for information relating to a serious crime
- To comply with Confidentiality Advisory Group approvals under Section 251 of the NHS Act 2006, which permits the collection of health information for patients with specific conditions without consent for the benefit of research and other important activities. Examples include the National Cancer Registry, the Trauma Audit and Research Network, the National Congenital Anomaly, Rare Disease Registration Service, and the NHS Patient Survey Programme. If you wish to opt out of your information being used for these purposes, please contact the Trust's Data Protection Officer.

Sharing information with your family

With your agreement we will share information about your current care with your family or carer. It is important that we know which family members or carers to involve in your care, and who we can share your information with. This person does not need to be related to you but they should be able to tell us your wishes in case you are unable to do so yourself.

Call recording

Telephone calls to Kettering General Hospital are routinely recorded to:

- Prevent crime or misuse
- Make sure that staff act in compliance with Trust procedures
- Ensure quality control and improve services
- Train staff.

CCTV

Security cameras are installed at various locations at the Kettering General site to prevent and detect crime, and for the protection of staff, visitors and patients and their property. Requests for copies of recordings should be directed to the Data Protection Administration Office³.

Short Message Service (SMS) text messaging

When attending the Trust for an outpatient appointment or a procedure you may be asked to confirm that the Trust has an accurate contact number and mobile telephone number for

³ See Useful Contacts

you. With your agreement your mobile number can be used to provide appointment details via SMS text messages.

Use of your information for other purposes

Relevant information about you may also be used to help us to:

- Receive funding and keep track of spending
- Teach and train our staff (but you can choose whether or not to be involved)
- Manage and plan our services
- Help investigate concerns or complaints that you or your family may have.

Wherever possible we use information that would not identify you personally (the information will be anonymised).

Using your information for research

Research has a vital role to play in the development of healthcare and health service delivery. The Trust is a proactive research institution and this is reflected in our aims and values. The Trust's Research and Innovation Department must approve research before it takes place. If we wish to use your personal information and health data for research, we would only do so with your explicit consent and will provide information beforehand regarding how your data will be processed.

How long do you keep my records?

There are national records management standards in the NHS for how long we need to keep information about you. This varies depending on the type of information. Typically, your health record is destroyed or deleted **8 years** following the end of treatment, or death. Records for some patients, e.g. children's records, are kept much longer. Our policy on the Retention and Disposal of Health Records is available upon request.

How do I update the personal information you have about me?

It is essential that we have your correct details to ensure the appropriate care, treatment and follow up is provided to you. If you change your name, address, phone number, or GP, please let our staff know so that your records can be updated. You should also tell us if any of your information we hold is incorrect.

How do we keep your information secure and confidential?

You have the right to confidentiality under data protection legislation, the Human Rights Act 1998 and the common law duty of confidence. Everyone working in the NHS has a legal duty to keep information about you confidential. Anyone who receives information from us is also under a legal duty to keep it secure and confidential.

Your information is held in secure systems in both paper and electronic format. Our electronic systems record when, and by whom, your record was accessed.

New systems are subjected to a data protection impact assessment (PIA) to ensure any risks to privacy are mitigated.

All staff complete annual data protection and confidentiality training, supplemented by related policies and procedures.

Transferring data abroad

Very occasionally your data may be transferred outside of the UK. If this is necessary for direct care purposes it is done so under contract, and a data processing agreement will stipulate the required protection required under data protection laws.

Your rights

GDPR affords patients, as data subjects, a number of rights in relation to the information we hold about them in health records, which are defined as a special category of personal data under GDPR. These rights are explained [here](#)⁴.

Upon request we will inform you whether your personal data is processed by the Trust and will send you a copy of that data. Click [here](#)⁵ to see the request form.

Useful contacts

Kettering General Hospital Data Protection Administration

Post: Data Protection Officer,
Rothwell Road
Kettering
NN16 8UZ

Tel: 01536 492000

Email:

Information Commissioner

If after exhausting our internal processes you believe that we have not complied with the data protection legislation you may wish to seek advice from the Information Commissioner.

Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Fax: 01625 524 510

Tel: 01625 545 700

Email: mail@ico.gsi.gov.uk

-- END --

⁴ See Appendix C

⁵ See Appendix B

APPENDIX B: ACCESSING YOUR HEALTH RECORD

1. WHO CAN ACCESS A HEALTH RECORD

The following are permitted to apply for access to the health record of a living⁶ patient:

- The patient.
- A person authorised in writing to make an application on behalf of the patient.
- A parent or guardian of a person under 16, if that person agrees or it is considered by the clinician to be in the patient's best interests.
- A Court appointed representative (Lasting Power of Attorney) (LPA) of someone who is not able to manage their own affairs. The LPA document must be registered with the Office of the Public Guardian.
- For any personal application not falling within one of these categories the Trust will require a Court Order.

2. MAKING A REQUEST

To confirm if the hospital holds any information about you as a patient, or to access your health record you should put your request in writing, preferably using the "Application to Access Health Records" form, which can be downloaded from our [website](#). Alternatively you can write to or telephone the Data Protection Administration Office on **01536 492412** and a form will be sent to you.

If you require access to your health record we will ask you to specify what documents or information you wish to have. This is because health records are often complex and may involve large amounts of information.

Completed forms should be sent to:

Data Protection Administration Office
Kettering General Hospital NHS Foundation Trust
Cytringan House
Robinson Way
Telford Way Industrial Estate
Kettering
Northamptonshire
NN16 8PT

3. DO I HAVE TO PROVE WHO I AM?

Yes, the Trust must be satisfied that an applicant is **the patient** or their **authorised representative**. This means we will ask for proof of identity and reserve the right to make further checks if necessary or refuse access if there is any doubt.

Applicants applying for a child's health records will be asked to supply a copy of the child's birth certificate and sign a form of authority confirming that they hold legal parental responsibility or if the applicant is not a parent, documentary evidence confirming parental responsibility.

⁶ A separate process exists to access the records of deceased patients under the Access to Health Records Act 1990.

4. CHILDREN AND YOUNG PEOPLE⁷

All individuals, including children, have the right of access to their personal information. They also have a right to confidentiality. A child will not always be able to make his or her own request, therefore when we receive an application from, or on behalf of a child, it is our obligation to judge whether the child understands the nature of the request. This is known as Fraser (or Gillick) competent. The hospital is obliged to take a child's view into consideration if he/she is Fraser competent as follows:

- Children aged 16 – 17 are regarded as adults and entitled to access their own personal information. Applications made on their behalf must be accompanied by their written consent.
- If the child aged under 16 does understand the nature of the request, he or she is entitled to exercise their own right of access, and in those circumstances we will reply to the child directly. Alternatively, a person with parental responsibility (as defined in the Children Act 1989⁸) can make an application on behalf of the child and a reply will can be sent to them directly.
- If the child does not understand, the person with parental responsibility is entitled to make a request and to receive a reply.

In all cases, the person with parental responsibility is only permitted to make such a request in the best interests of the child, not in their own interests.

5. DO I HAVE TO GIVE A REASON WHY I WANT THEM?

You do not have to explain why you want to access records unless it is in relation to commencing clinical negligence proceedings.

6. HOW LONG WILL IT TAKE?

We process ALL applications in strict date of receipt order. We are unable to provide an immediate response to applications or to fast track applications. We will always try to provide copies of the records requested within **one month**. If your request is complex or the records/data involved is very large we may write to you to apply a time extension to your case. We will explain why this is necessary.

7. HOW MUCH DOES IT COST?

A copy of a health record is provided free of charge. However, we may apply a charge if we consider your request to be manifestly unfounded or excessive,

⁷ Section may need updating in response to the new UK Data Protection Act and clarification of age of capacity.

⁸ The *Children Act 1989* sets out who has parental responsibility and includes:

- The child's parents if married to each other at the time of conception or birth;
- The child's mother, but not father if they were not so married *unless* the father has acquired parental responsibility via a court order or a parental responsibility agreement or the couple subsequently marry;
- The child's legally appointed guardian – appointed either by a court or by a parent with parental responsibility in the event of their own death;
- A person in whose favour a court has made a residence order concerning the child;
- A local authority designated in a care order in respect of the child (but not where the child is being looked after under section 20 of the *Children Act*, also known as being 'accommodated' or in 'voluntary care');
- A local authority or other authorised person who holds an emergency protection order in respect of the child.

particularly if it is repetitive or in relation to additional copies of information already provided. If we advise you that a fee is payable, the cost will be calculated on the administrative cost to us of providing the information.

8. HOW WILL I RECEIVE THE RECORDS?

Electronically-held records

Many of our records are now held electronically and supplied in their original digital format on a password protected CD. A large volume of paper records have also been scanned and held electronically. You will receive the password to the CD in a separate letter to you in order to ensure your records are secure in transit.

Paper records

These are supplied as paper photocopies.

Delivery

Records will be forwarded to you using the Royal Mail's 'Special Delivery' service, which requires a signature upon receipt.

9. ARE THERE ANY EXCEPTIONS?

If healthcare professionals believe that information within records would cause serious harm to the physical or mental health of the patient or another person, they are entitled to refuse access to some or all records. Access may also be withheld or limited if the records relate to and identify another person other than a health professional.

If you are applying for the records of another party you will not be allowed to access any information which the patient gave on the understanding that it would remain confidential or was not to be disclosed to the applicant. If access to the record is refused, the healthcare professional is not required to tell you the reasons why.

If you are a parent or a person with parental responsibility for a child or young person who may not see their own record and the healthcare professional believes it is not in the best interests of the child for you to see the health record.

10. WHAT IF I CANNOT READ THE RECORDS OR UNDERSTAND THEM?

If necessary, we will contact the healthcare professional concerned and ask for an explanation of any unfamiliar terminology used or a typed transcript of that part of your record, or possibly arrange a meeting with you to discuss any difficulties you may have with understanding the information.

-- END --

APPENDIX C: INFORMATION FOR PATIENTS

Your rights under the General Data Protection Regulation

1. **The right to be informed** – this encompasses our obligation to provide fair processing information, which we do through a privacy notice, click [here](#)⁹.

2. **The right of access** – this is your right to obtain confirmation that we process your data and access to it.

For details about how to obtain confirmation that we process your data and/or to access your personal health data, please click [here](#)¹⁰.

3. **The right to rectification** – this is your right to have your personal data rectified if it is inaccurate or incomplete. If you believe that the information recorded about you is incorrect, you will need to tell us so that we are able to contact the person who entered the information. We will correct factual mistakes and provide you with a copy of the corrected information. Wherever possible, we will also tell you the names of any third parties that we have disclosed this data to.

If you are not happy with an opinion or comment that has been recorded, we will add your own comments to the record so they can be viewed alongside any information you believe to be incorrect.

4. **The right to erasure** – this is also known as your ‘right to be forgotten’, where there is no compelling reason to continue processing your data in relation to the purpose for which it was originally collected or processed.

Your health record is retained in accordance with NHS national guidance, and because of our legal obligation to keep health records, it is extremely rare that we destroy or delete records earlier than the recommended retention period. However, if you believe you have compelling grounds for having all or part of your record erased you should contact our [Data Protection Officer](#)¹¹.

The clinician in charge of your care and our Caldicott Guardian will decide whether we can safely accommodate your request. If you are unhappy with our decision you may wish to register a complaint to the [Information Commissioner](#)¹².

5. **The right to restrict processing** – this is your right to block or suppress the processing of your personal data. If you raise an issue relating to your health record that requires us to restrict processing, we will put an alert on our main patient system to flag that we are investigating your concerns. Please note it will not be possible to restrict processing while you are receiving care and treatment at the hospital.

6. **The right to data portability** – this is your right to obtain and re-use any information you have provided to us as part of an automated process. At present we do not process any personal data that meets this requirement.

⁹ Link to Appendix A.

¹⁰ Link to Appendix B.

¹¹ See Useful Contacts.

¹² See Useful Contacts.

7. **The right to object** – this is your right to object to the hospital processing your health data because of your particular situation. Because of our legal obligation to keep health records it is extremely rare that we would stop processing your data if you wish to continue to be treated by the hospital. If you believe you have compelling grounds for the hospital to stop processing your data you should contact our Data Protection Officer.

The clinician in charge of your care and our Caldicott Guardian will decide whether we can safely accommodate your request. If you are unhappy with our decision you may wish to register a complaint to the Information Commissioner.

8. **Rights in relation to automated decision making and profiling** – GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. While the hospital uses systems, such as an Early Warning Score to determine how well a patient is, it does not replace our staff's clinical judgements when making decisions about your care.

If you wish to know more about how these systems work, please contact our Data Protection Officer.

Useful contacts

Kettering General Hospital Data Protection

Post: Data Protection Officer,
Rothwell Road
Kettering
NN16 8UZ
Tel: 01536 492000
Email: dpokettering@nhs.net

Information Commissioner

If after exhausting our internal processes you believe that we have not complied with the data protection legislation you may wish to seek advice from the Information Commissioner.

Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF
Fax: 01625 524 510
Tel: 01625 545 700
Email: mail@ico.gsi.gov.uk

-- END --

APPENDIX D: EMRAD PRIVACY NOTICE

What is EMRAD?

EMRAD is the East Midlands Radiology Consortium which aims to deliver timely and expert radiology services to patients across the East Midlands, regardless of where they are being treated. Radiology services include imaging tests like x-rays and scans.

The EMRAD network comprises the following Acute NHS Trusts:

- Burton Hospitals
- Chesterfield Royal Hospital
- Derby Teaching Hospitals
- Kettering General Hospital
- Northampton General Hospital
- Nottingham University Hospitals
- Sherwood Forest Hospitals
- United Lincolnshire Hospitals

A key benefit for patients is that clinicians, and other staff who support your care, can access your complete radiology imaging record, including scans, reports and clinical opinions, regardless of where they are based in the East Midlands, which enables clinicians to provide more care closer to patients' homes.

It will also help to avoid unnecessary appointments and duplicate or repeat scans.

What personal information is captured?

In addition to your demographic information (name, address, GP, etc) the system stores images from all radiology tests you undergo at any of the EMRAD hospitals. It also stores all radiology reports for these tests and records patient dose¹³, and protocol information, using a system called DoseWatch, for procedures using X-rays.

How long are records kept?

There are national records management standards in the NHS for how long we need to keep information about you. This varies depending on the type of information. Typically, a patient's health record is destroyed or deleted **8 years** following the end of treatment, or death. Records for some patients, e.g. children's records, are kept much longer.

Who can access my information?

Only those involved in providing or supporting your care are able to access your information. Your information will not be shared with anyone else, unless there is a clear legal basis for doing so, for example, with your explicit consent.

EMRAD has implemented FairWarning's Patient Privacy Intelligence™, which is a leading compliance and information security platform to provide assurance for the privacy and

¹³ DoseWatch information is used for clinical audit and the optimisation of clinical images acquired within imaging departments. Clinical imaging and scientific staff will only have access to information relevant to their work. The information is analysed by clinical scientists or clinical imaging staff and is used to feed back to clinical staff on their use of imaging equipment and patient exposures.

confidentiality of patient health information in the EMRAD GE PACS application, in particular to proactively audit whether user access to patient records is legitimate. In doing so, EMRAD uses the FairWarning Patient Privacy Intelligence solution to help demonstrate compliance with data protection legislation.

Do I have a choice about who can access my information?

If you wish to restrict who can access your information it is possible that an imaging examination will not be able to be performed in an EMRAD hospital. However, all events in the EMRAD system are logged so we can see who accesses your record, when, and what changes were made. If you have any concerns about who is accessing your radiology information you can contact the Radiology Department at your local hospital.

Is my information safe?

By law all healthcare staff must keep your information secure and confidential. Your rights are protected under data protection legislation. The systems we use in the NHS comply with stringent levels of safety, security and confidentiality.

What are my rights?

1. **The right to be informed** – this encompasses our obligation to provide fair processing information, which we do through this privacy notice.
2. **The right of access** – this is your right to obtain confirmation that we process your data and access to it. For details about how to obtain confirmation that we process your data and/or to access your personal health data, please contact your Trust's Data Protection Officer.
3. **The right to rectification** – this is your right to have your personal data rectified if it is inaccurate or incomplete. If you believe that the information recorded about you is incorrect, you will need to tell us so that we are able to contact the person who entered the information. We will correct factual mistakes and provide you with a copy of the corrected information. Wherever possible, we will also tell you the names of any third parties that we have disclosed this data to.

If you are not happy with an opinion or comment that has been recorded, we will add your own comments to the record so they can be viewed alongside any information you believe to be incorrect. If you have any concerns about the accuracy/ completeness of your EMRAD records, please contact your Trust's Data Protection Officer.

4. **The right to erasure** – this is also known as your 'right to be forgotten', where there is no compelling reason to continue processing your data in relation to the purpose for which it was originally collected or processed.

Your health record is retained in accordance with NHS national guidance, and because of our legal obligation to keep health records, it is extremely rare that we destroy or delete records earlier than the recommended retention period. However, if you believe you have compelling grounds for having all or part of your record erased you should contact your Trust's Data Protection Officer.

The clinician in charge of your care and our Caldicott Guardian will decide whether we can safely accommodate your request. If you are unhappy with our decision you may wish to register a complaint to the Information Commissioner.

5. **The right to restrict processing** – this is your right to block or suppress the processing of your personal data. If you raise an issue relating to your health record

that requires us to restrict processing, we will put an alert on our main patient system to flag that we are investigating your concerns. Please note it will not be possible to restrict processing while you are receiving care and treatment.

6. **The right to data portability** – this is your right to obtain and re-use any information you have provided to us as part of an automated process. At present EMRAD does not process any personal data that meets this requirement.
7. **The right to object** – this is your right to object to the hospital processing your health data because of your particular situation. Because of our legal obligation to keep health records it is extremely rare that we would stop processing your data if you wish to continue to be treated by the hospital. If you believe you have compelling grounds for the hospital to stop processing your data you should contact your Trust's Data Protection Officer.

The clinician in charge of your care and our Caldicott Guardian will decide whether we can safely accommodate your request. If you are unhappy with our decision you may wish to register a complaint to the Information Commissioner.

8. **Rights in relation to automated decision making and profiling** – GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. At present this does not apply to EMRAD.

Useful contacts

EMRAD Trust	Data Protection Officer
Burton Hospitals	Anne Woodhouse, anne.woodhouse1@nhs.net
Chesterfield Royal Hospital	[TBC]
Derby Teaching Hospitals	Anne Woodhouse, anne.woodhouse1@nhs.net
Kettering General Hospital	Neill Bolderston DPOkettering@nhs.net
Northampton General Hospital	[TBC]
Nottingham University Hospitals	Rory King, DPO@nuh.nhs.uk
Sherwood Forest Hospitals	Jacqui Widdowson, jacqui.widdowson@nhs.net
United Lincolnshire Hospitals	[TBC]

Information Commissioner	<p>Post: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF</p> <p>Fax: 01625 524 510</p> <p>Tel: 01625 545 700</p> <p>Email: mail@ico.gsi.gov.uk</p>
--------------------------	--