King’s College Hospital
NHS Foundation Trust
Privacy Notice

Version 3.0

June 2025

Contents

1 Introduction

King’s College Hospital NHS Foundation Trust (the Trust) works within the NHS Constitution and in line with the NHS’s values, which place patients at the heart of everything the NHS does.

- Further information about the NHS Constitution can found at https://www.gov.uk/government/publications/the-nhs-constitution-for-england/
- The Trust is also a member of King’s Health Partners (KHP)which is an Academic Health Sciences Centre. Further information can be found at http://www.kingshealthpartners.org
- The Trusts is also a member of the Our Healthier South East London Integrated Care Services (OH SEL ICS). Further information can be found at Welcome | Our Healthier South East London (ourhealthiersel.nhs.uk)

2 Freedom of Information

The Trust is a public authority as defined by the Freedom of Information Act (FOIA).

- It will ensure that any patient-related data provided under the FOIA is only released where allowed by law and anonymised within context.

3 Trust Oversight

The Trust and its Board are supported by a number of key roles. These include:

- the **Senior Information Risk Owner (SIRO)**, who is accountable to the Board with regards to information risk management including Information Governance
    - Contact email is kch-tr.siro@nhs.net
- the **Caldicott Guardian (CG)**, who advises on specific issues relating to the use of Personal Confidential Data (PCD)
    - Contact email is kch-tr.cladicottqueries@nhs.net
- the **Data Protection Officer (DPO)**, who advises on the legal basis for the use of Personal Confidential Data (PCD) and compliance with current Data Protection Legislation
    - contact email is kch-tr.dpo@nhs.net

4 Definitions

4.1 What is Personal Confidential Data?

This is a term defined in the Caldicott Information Governance Review 2013. It describes personal information about identified or identifiable individuals that should be kept private or secret and includes deceased NHS Patients (only NHS patients) as well as living people.

The review interprets 'personal' as including the Data Protection Act 2018 definition of personal data but includes data relating to the deceased as well as living people. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'sensitive', as defined in the Data Protection Act.

Examples of identifiable data are:

- Name
- Address
- Postcode
- Date of birth
- NHS Number (which is now a legal requirement to share for direct care purposes as a consequence of the Health & Social Care Act 2015)
- Car Registration Number
- Internet Protocol (IP) Address

4.2 What is Personal Data?

The definition used comes from the Data Protection Act 2018 and is further defined by the Information Commissioner's Office (ICO).

Personal Data means data which relate to a living individual who can be identified:

(a) from those data, or

(b) from those data and other information, which is in the possession of, or is likely to come into the possession of, the Controller. (Under the UK General Data Protection Regulations, this means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by State laws.) It includes any expression of opinion about the individual and any indication of the intentions of the Controller or any other person in respect of the individual.

4.3 What are Special Category Data?

Special Category Data are different from Personal Data. They are specific data points consisting of information about the data subject's:

(a) racial or ethnic origin

(b) political opinions

(c) religious beliefs or other beliefs of a similar nature

(d) membership of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992)

(e) physical or mental health or condition

(f) sexual life

(g) criminal data such as commission or alleged commission of any offence, or any proceedings for any offence committed or alleged to have been committed, the disposal of such proceedings or the sentence of any court in such proceedings.

(h) employment and social security

(i) biometric / genetic information

4.4 Protected Characteristics

Protected characteristics are aspects of a person’s identity that makes them who they are. Everyone has at least of few of the nine protected characteristics, so as an employer, it’s important you make sure an employee isn’t treated less favorably because of theirs.

Originally, there were various pieces of legislation in place that protected people from discrimination based on various characteristics of their identity – these included the Sex Discrimination Act 1975, the Race Relations Act 1976 and the Disability Discrimination Act 1995, to name just a few. However, in 2010, the Equality Act 2010 replaced these multiple pieces of legislation in an attempt to simplify the law and bring together all anti-discrimination legislation under one Act.

There are nine characteristics outlined in the Equality Act 2010 which are:

- Age
- Gender
- Race
- Disability
- Religion or belief
- Sexual orientation
- Gender reassignment
- Marriage or civil partnerships
- Pregnancy and maternity

4.5 How is Direct Patient Care defined?

The Caldicott Review defines it as a clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society.

It includes the assurance of safe and high-quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction, including measurement of outcomes undertaken by one or more registered and regulated health or social care professional and their team with whom the individual has a legitimate relationship for their care.

Primary use data is information / data generated through and used for the provision of direct patient care (not to be confused with primary care data, which is created, used and shared from GP practices and similar organisations).

4.6 How is Indirect Patient Care defined?

The Caldicott Review defined it as activities that contribute to the overall provision of services to a population as a whole or to a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine and medical research. Examples of activities include risk prediction and stratification, service evaluation, needs assessment and financial audit.

This is also called secondary use data (not to be confused with secondary care data, which is created, used and shared from acute trusts and similar organisations).

4.7 Information Commissioner’s Office Definitions

The Information Commissioner’s Office (ICO) has further definitions from the Data Protection Act 2018 at https://ico.org.uk/for-organisations/guide-to-data-protection/keydefinitions

4.8 What Information do we process

The Trust may process information in relation to things such as:

- staff administration
- accounts and records (including debt collection, collection of fees linked to overseas visitors, cross border i.e. patients whose treatment is funded by Scottish, Welsh and Northern Irish health bodies)
- health administration and services (defined by statute and contract)
- research and innovation
- crime prevention and prosecution of offenders
- public health
- data matching, which involves comparing computer records held by one body against those held by the same or another body to see how far they match. When a match is found it may indicate that there is an inconsistency which will then require further investigation.
- advertising, marketing and public relations
- administration of Membership records
- education
- fundraising
- pastoral care
- property management
- processing for not-for-profit organisations.

We also process sensitive classes of information that may include: • racial and ethnic origin • offences (including alleged offences), criminal proceedings, outcomes and sentences • trade union membership • religious or similar beliefs • employment tribunal applications, complaints, accidents and incident details • ordinary country of residence and nationality

It may sometimes be necessary to transfer personal information overseas. When this is required, information may be transferred to countries or territories around the world. Any transfers will be made in full compliance with all aspects of current DPA legislation.

5 Why we collect information about you

In carrying out our roles and responsibilities as an employer and a provider of services for people working and living in its catchment area, it is essential that the Trust has an understanding of the health and social care needs of the local and wider community to ensure that appropriate services are identified and made available across our responsible area and nationally as required.

This means we need to use information about our patients for direct clinical care and to understand how services should be provided.

We do not, however, need to have and use all the information that is available and provided for purposes other than the provision of direct care.

Where excessive data is identified, information is either removed or de-identified (a form of anonymisation) prior to subsequent reuse.

We may keep your information in written format and/or in digital format, and your record will include basic details about you, such as your name and address, and may also contain more sensitive information about your health and social care conditions, usage of current services and details such as outcomes of needs assessments.

6 How your information is used to help the wider NHS

Your anonymised information will be used to help assess the needs of the general population and support the Trust in making informed decisions about the provision of future services. Information can also be used to conduct health research (see http://www.hra.nhs.uk) and to develop and monitor NHS performance.

Where information is used for statistical purposes, stringent measures are taken to ensure individual patients cannot be identified. Anonymous statistical information may also be passed to organisations with a legitimate interest, including universities, community safety units and research institutions.

7 Why we keep your information confidential and safe

It is everyone's legal right to expect that information held and used about them is safe and secure and is only used for the agreed purpose(s).

Everyone working for the NHS is subject to the Common Law Duty of Confidentiality (https://www.health-ni.gov.uk/articles/common-law-duty-confidentiality). Information provided in confidence will be used only for the provision of direct care or for the purpose(s) advised with consent given by the patient, unless there are other specific circumstances covered by current UK and European legislation.

The Trust takes this responsibility very seriously and has ensured that it has robust and effective measures, processes and procedures in place to achieve this expectation for you and the information we hold and process about you.

Supporting this approach, under UK law, NHS guidance and directions such as the Common Law Duty of Confidence and the NHS Confidentiality Code of Conduct, all our staff are also required to protect your information, tell you how your information will be used, and enable you to decide if and how your information can be shared.

The Trust has incorporated the NHS England Guide to Confidentiality into its daily working practice.

This guide is available at https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/a-guide-to-confidentiality-in-health-and-social-care

8 Processing your Personal Data

8.1 Mechanisms for processing your Personal Data

The Trust processes Personal Data for a number of reasons in various ways. These are outlined below:

- **For the purpose of direct patient care**, the Trust will ensure that any information collected about you is initially provided by you, and where any additional information is collected or used, it will be with your explicit consent for that purpose or activity.

- **For the purpose of internal operations (System Management)**, the Trust will use both electronic and manual mechanisms to process personal confidential information relating to its employees and visitors to our sites and services. This is based on explicit consent provided by each employee at the time of joining and updated when any changes are made through internal communications.

- **For the provision of indirect care**, and to maintain rules for use of information, the Trust uses a number of approved and secure services / systems to process information about you.

- **For the provision of Research and Development,** the Trust is a major research center and engages in a wide range of research projects to support and develop clinical improvements working with other NHS bodies, academic centers and other key partners both in the Uk and internationally.

8.2 How Personal Data Is used within our Systems

If you are receiving care from any health or care organisation, that organisation may share your NHS number with other organisations providing your care. This is so that the health and care organisations are using the same number to identify you whilst providing your care. By using the same number, the health and care organisations can work together more closely to improve your care and support.

Your NHS number is accessed through an NHS England service called the Personal Demographic Service (PDS). A health or Social care organisation sends basic information such as your name, address and date of birth to the PDS in order to find your NHS number. Once retrieved from the PDS, the NHS number is stored in our case management system (Epic). These data points are retained in line with our record retention policies and in accordance with the Data Protection Act 2018, Government record retention regulations and best practice. Further information is available on our website.

We will share further health information only to provide those health and care professionals directly involved in your care access to the most up-to-date information about you. Access to information is strictly controlled, based on the role of the professional, and where the user has a direct care relationship with you.

You have the right to object to the processing of your NHS number in this way. This will not stop you from receiving care but will result in the benefits outlined above not being realised. To help you decide, we will discuss with you how this may affect our ability to provide you with care, and any other options that you have.

9 Data Protection and Confidentiality

The Data Protection Act (DPA) came into force in May 2018. It places a responsibility on the Trust as a Controller to ensure that your information is collected and managed in a secure and confidential way (Data Protection registration number Z4653019).

The DPA also provides you with a number of rights about how your information is used by us, which are;

2. **Right to be informed** - Individuals have the right to be informed about the collection and use of their personal data. This is completed by this notice and supporting leaflets, posters available in the Trust and discussions with our clinical and corporate teams.
3. **Right of access** - right to access and receive a copy of their personal data, and other supplementary information right of access to personal information that the Trust holds about you. (This applies equally to service users, members of staff and any other individual that the Trust may hold information about in its legal capacity.) Requests for access to personal information we hold about you are called Subject Access Requests – see below for more information.
4. **Right to rectification** -right for individuals to have factually inaccurate personal data rectified or completed if it is incomplete.
5. **Right to erasure** - right for individuals to have personal data erased (Also known as right to be forgotten). This does not apply to clinical opinion recorded within in the records.

6. **Right to restriction** - right to request the restriction or suppression of their personal data.
7. **Right to data portability** - allows individuals to obtain and reuse their personal data for their own purposes across different services.
8. **Right to Object** – allows individuals the right to object to the processing of their personal data in certain circumstances. This should be discussed with relevant clinical teams if requested.
9. **Rights in relation to automated decision making and profiling** – allows individuals the right to restrict the use of their information where decisions are being made fully automated or used for profiling.

You can find full details of the DPA at http://www.legislation.gov.uk/ukpga/2018/29/contents
The Trust also issues an annual report on its Information Governance compliance including its annual NHS England assessment called Data Security and Protection Toolkit (DSPT). This identifies what governance and controls it has in place in line with legal and national guidance (https://www.dsptoolkit.nhs.uk/).

10 How will we use information about you?

Your information is used to run (Clinical Care) and improve (Service Development) the Trust and the services that it provides. It may also be used to:

A. check and report on how effective the Trust has been in providing direct services to patients and the community and any services it has commissioned from other providers

B. ensure that money is used properly to pay for the services it provides (Service Quality)

C. investigate complaints, legal claims or serious incidents (Legal Compliance)

D. make sure that the Trust delivers value for money (Clinical Audit)

E. make sure services are planned to meet patients' needs in the future (Service Planning)

F. review the care given to make sure it is of the highest possible standard (Service Evaluation)

G. where the Trust has been commissioned to provide specialised services (Service Evaluation and reporting)

H. improve the efficiency of healthcare services, by sharing information with other organisations (sometimes non-NHS) for a specific, legally justified purpose (Service Research and Development)

I. support the Trust when seeking reimbursement for treatment that has been provided (the amount of information used will be the minimum necessary) (Finance)

J. fulfil contractual obligations as set out in the NHS Standard Contract. (Commercial Obligations)

11 Information sharing with other NHS agencies and non-NHS organisations

To support our own functions and the wider OH SEL ICS services, we share your information for health purposes and for your benefit with other organisations such as NHS England, other NHS organisations etc.

We may also need to share information with our partner organisations, such as King's Health Partners as part of our research and service development programs.

Where necessary or required we may also share information with:

- our patients
- family, associates and representatives of the person whose personal data we are

processing

- staff
- current, past or potential employers
- healthcare social and welfare organisations
- suppliers, service providers, legal representatives
- auditors and audit bodies
- educators and examining bodies
- survey and research organisations
- people making an enquiry or complaint
- financial organisations
- professional advisers and consultants
- business associates
- police forces
- security organisations
- central and local government
- voluntary and charitable organisations
- professional regulatory bodies.

11.1 Information may also need to be shared with other non-NHS organisations.

Where information sharing is required with third parties outside of normal clinical reasons, we will always have a relevant contractual obligation and Data Sharing Agreement (DSA) in place.

There are exceptions to this requirement such as where there are clear and exceptional clinical reasons to share (Health and Social Care Act – Section 251 (b) – Duty to share information in the vital interests of the individual)

We are required by law to report certain information to the appropriate authorities. This is only provided after formal permission has been given by a qualified health professional. Examples of the occasions when we must pass on information, are

- notification of new births
- notification of infectious diseases which may endanger the safety of others, such as meningitis or measles (but not HIV/AIDS), and
- where a formal court order has been issued.

11.2 Our guiding principle is that we are holding your information in the strictest confidence.

We may be asked to share basic information about you, such as your name and address which does not include sensitive information where the Trust holds such information. This would normally be to assist another organisation to carry out their own statutory duties. In these circumstances, where it is not practical to obtain your explicit consent, we will inform you through a Privacy Notice (such as this one), under the Data Protection legislation.

12 Significant Sharing your information

Kings College Hospital is involved in a number of key programs that support and require the sharing of your data with different bodies to support your care. The key programs are outlined below;

12.1 Electronic Health Record (Epic)

We have teamed up with Guy's and St Thomas' NHS Foundation Trust and implemented in 2024 our new electronic health record Epic. This single system is used by both Trusts (and also Synnovis who provide pathology services) to provide our care for you.

In addition, the system which is also used in a variety of other NHS Trusts across England and Norther Ireland has the capability to share information across the system (Attend Everywhere) automatically between locations allowing our clinical teams access to the most current information in the provision of your care.

Your records will be accessed only by the clinical staff directly involved in your care at these hospitals.

12.2 Integrated Care Records:

Integrated care records are a key development where we and other NHS and Social Care services share information between each to support your direct care and help the organisation to provide the best possible services. Kings are currently involved in a number of these projects such as.

12.2.1 **London Care Record** - this is a new service and has a wider engagement with all health and social care services across London and adjacent regions. This program will support and enable clinicians and relevant clinical care teams looking after you to support your care across the London Health Economy. Further details are available at the following web site - https://www.ourhealthiersel.nhs.uk/privacy-notice.htm

To opt out of this service please contact the Trust Data Protection Officer (kch-tr.dpo@nhs.net) in the first instance.

12.3 London Data Services

This is a key program of work that currently brings together organisations across South East London, North West London and North East London. We are collaborating with others across London to create a data service which will help with the planning of people's care and the design of new services. These capabilities will improve professionals' ability to predict illness and disease (Risk Stratification), allow services to manage demand and capacity, ensure that resources are centered on the right need areas and much more (Service Planning). It will also help to advance research into new health and care services and medical advances such as drugs and new treatments.

Further details of this service and an explanation of how you can opt out of your data being used in this service are available at https://www.ourhealthiersel.nhs.uk/privacy-notice.htm

Care professionals will be able to work together even more closely on designing and delivering better joined-up care to the whole population and identify those most at risk of illness or rising need. The video below helps to explain some of the benefits of such an approach:

12.4 Kings Health Partners

We have teamed up with Guy's and St Thomas' NHS Foundation Trust and the South London and Maudsley NHS Foundation Trust in a partnership known as King's Health Partners (https://www.kch.nhs.uk/about/the-kings-story/partnership-working), an Academic Health Science Centre. We are working together to give our patients the best possible care, so you might find we invite you for appointments at these hospitals. To make sure everyone you meet always has the most up-to-date information about your health, we may share the information in your medical records between these hospitals using a secure system called KHP Online.

Your records will be accessed only by the clinical staff directly involved in your care at these hospitals and not for research or other non-clinical purposes. If you do not want your records to be available in this way, please contact gst-tr.GSTPALS@nhs.net.

13 Your right to withdraw consent

The Trust has its own local consent / opt-out processes and mechanisms for allowing information not to be shared or to be restricted. However, it must be emphasised that this cannot be totally restricted and at times consent may be overridden, especially in relation to matters such as safeguarding children/vulnerable adults, female genital mutilation (FGM) or the correct charging for services provided by the NHS.

Where you wish to restrict your information across the NHS, generally the process is the same for local and national schemes: you can opt out at any time by speaking to your GP practice reception.

But please be clear about which scheme you want to opt out of.

13.1 What is the patient opt-out?

UK DPA Legislation provides the right to “opt out” of the use of persona data in limited uses. In addition, the NHS Constitution states: “You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered.” These are two very different aspects of how your personal data is used.

We recognise that you may want to prevent confidential information about you from being shared or used for any purpose other than providing your care. IN most cases we will discuss with you the benefits to you and will try to respect your wishes unless one of the following criteria applies, which means that it is not possible to opt out of having your information shared:

- the information is essential to support your direct care and treatment between individual organisations

- you have consented to the use of your information (whether before or after registering a National opt-out statement – see below for explanation) for a specific purpose such as research.

- a mandatory legal requirement (such as a court order) exists.

- the information released is not considered to be identifiable personal confidential data. This is called Anonymised data (in line with the Information Commissioner’s Office Code of Practice)

- the information is used to support the management of communicable diseases and other risks to public health under Regulation 3 of the Health Service (Control of Patient Information) Regulations 2002.

There are several forms of opt-outs available at different levels. These include, for example:

- information directly collected by the Trust. Your choices can be exercised by withdrawing your consent for the sharing of information that identifies you, unless there is no overriding legal obligation (Local Opt Out)

- information not directly collected by the Trust but collected by organisations that provide NHS services. (Type 1 and National Data Opt Out)

13.2 Type 1 opt-out

This is a General Practice standard and ONLY applies to General Practices. If you do not want personal confidential data / information that identifies you to be shared outside your GP practice, for purposes beyond your direct care you can register a type 1 opt-out with your GP practice. This prevents your personal confidential information from being used other than in particular circumstances required by law, such as a public health emergency like an outbreak of a pandemic disease.

Records for patients who have registered a type 1 opt-out will be identified using a particular code that will be applied to your medical records, and which will stop your records from being shared outside of your GP practice.

13.3 Local Opt Out

This is a local process to register a wish to control the sharing of personal data from Kings College Hospital.

13.4 National Data Opt Out (NDOO)

This was introduced following the National Data Guardians report in 2013and implemented in 2018. This is used to determine those data subjects that decide to register a statement with NHS England to prevent the use of their data for secondary uses (e.g. Service development and Research). Further details can be found at https://digital.nhs.uk/services/national-data-opt-out . This link also is the location to register your wishes.

14 Private healthcare

This Trust allows or undertakes private healthcare treatment from its premises.

As such, it must comply with the Competition & Markets Authority Order linked to the sharing of data to support a number of functions.

This requires the data to be linked to your NHS Number, and you may be asked to disclose this. You are under no obligation to do so, and should you decide not to disclose it this will not impact on the care or services you receive from the Trust.

Further information about this can be found at https://www.phin.org.uk/#!/ .

15 Accessing the information about you held by the Trust

Under the Data Protection Act 2018 you have the right to see or be provided a copy of the Personal Data held about you. To gain access to your information you will need to make a Subject Access Request (SAR) to the Trust – please see the following link https://www.kch.nhs.uk/search?query=subject+access+request

Ther is no charge for requests for paper records, electronic records, x-rays and other imaging, but we can charge for medical reports or some administration costs. In all cases, we will provide notice if any costs are applicable. In line with all NHS organisations, we comply with the NHS England Records Management Code of Practice for Health and Social Care 2023 (https://transform.england.nhs.uk/information-governance/guidance/records-management-code/).

Please note that this guidance not only defines the minimum period an organisation should keep information for but also when it can be legitimately destroyed. That means there may be occasions where the Trust no longer holds data because their retention was no longer required in line with this guidance.

Data may be destroyed via a combination of methods depending on how the information has been stored and which organisations may have been processing data on behalf of the Trust.

If you wish to make a SAR, please email the Subject Access Team at kch-tr.SubjectAccessRequestsDH@nhs.net

16 Where to get further Information

If you wish to complain about anything in this Privacy Notice, please contact us via the PALS email kch-tr.pals@nhs.net.

For further information on how to access your records, please go to the “How can I see my records?” section on our Patient Information page at https://www.kch.nhs.uk/patientsvisitors/patients/what-you-need-to-know/patientinformation

Disclaimer: please note that we cannot take responsibility for the content of external, non-King's College Hospital Foundation Trust websites.

Appendix 1 – Research

Use of Data for Research

King's College Hospital NHS Foundation Trust, like almost all NHS organisations, participates in and supports health and social care research. During any research study that you have agreed to participate in, information about you is collected in order to conduct the study and for analyses. On some occasions information that has already been collected for your normal care is then re-used for research purposes.

For more details on the use of information in research please see the Health Research Authority's website and the National Data Guardian website.

We have also compiled a list of frequently asked questions about the use of data in research:

How your information may be used

- What patient information do you keep?

Whenever you visit the hospital, information is collected about you and stored in a number of places. This is called your NHS health (also known as medical) record. This includes basic information such as your name and address as well as results of any tests, such as your blood pressure readings or results of x-rays. We call all of this information 'Routinely Collected'.

- How is my routinely collected information used in the hospital?

Routinely collected information is used to help your medical team to decide on the best way to look after you. It is also used to support clinical audits (reviews of a large number of patients' health records) to help identify ways to improve overall care in the hospital.

Your information is also used for a number of other purposes such as national health registries, patient surveys and medical research.

- How is my information used for medical research?

Researchers use information to increase our understanding of diseases and improve treatment. Before any research is conducted it usually requires approval from an independent ethics committee who will ensure that any patient information is being used ethically and appropriately.

In almost all cases, information is collected for a particular research study in addition to your routinely collected information. This information would be kept by individual research teams securely in a special database for that study. To participate in a research study, you will usually be required to provide consent. In most cases, you will be requested to sign a consent form. Any consent forms with your signature and personal details are stored by the research teams in a secure location along with the study information.

- Do you keep personal information?

Usually, information for research is fully or partially anonymised (de-identified). Any personal details such as your name, address and NHS number are removed, and a study reference number is assigned to your study information.

- Do you use my information for research without my consent?

Occasionally some studies will use your routinely collected information for research without your consent. For researchers to use any patient information without consent, it must either be completely anonymous to anyone outside of your direct care team or the researcher may need to apply for permission from a group called the Confidentiality Advisory Group. This is in line with the UK research governance framework Health Research Ethics Committees: Governance Arrangements.

A list of studies which are approved to do this is available on the HRA website.

All research involving NHS patients requires approval from the hospital where the research is taking place. This approval is issued by the Research and Innovation department who ensure that all applicable approvals are in place for the research to commence.

- ## Why is it beneficial to use routinely collected information?

By using routinely collected information, researchers can conduct data analysis without involving or contacting patients. Researchers can include more patient data which can improve the accuracy of the results, and speed up the translation of improvements to care and treatment for patients to experience in clinics.

- ## Will it affect my care?

If the information is completely anonymous there will be no way for the researcher to know who you are and therefore your care will not be affected at all.

If the information is partially anonymised and the researcher identifies something in the data about you which may be important, they are obliged to inform your care team.

- ## Will you share my information with other organisations?

For some research projects, we share information with other hospitals and vice versa so that we and they have access to even more information. These are called multi-centre research studies which help us improve the quality of research by covering a larger section of the population.

Occasionally we will be contracted by a commercial company such as a pharmaceutical company to carry out a research study on their behalf. This may involve testing a new drug or device that they have developed. The information that comes from these studies is given to the company so that they can do things like assessing their product's safety or to help them to market the product. Your consent is required to share your data with commercial organisations and external organisations.

When we collaborate with private companies, the aim is always to benefit patients and the NHS.

We will never share your information with insurance companies without your consent.

- ## Can I opt out of sharing my information?

You have the right to object to the use of your information for any purpose other than your own medical care. If you do this, we will exclude your information wherever we can.

There are several levels of opt-out you can choose, you can:

1) opt-out of research and data sharing at a national-level

- See National Data Opt-out Programme

2) opt-out of data sharing with the local care record

- See Local Care Record

3) opt-out of data to be used for research

- Contact the KERRI team on kch-tr.cogstackrequests@nhs.net

To request a copy of your own health records, please refer to the link:
https://www.kch.nhs.uk/patientsvisitors/patients/what-you-need-to-know/patient-information

In some instances, we are unable to remove your data, for example if your data has already been anonymised or if your information is needed for drug safety data.

Further information

We hope this information has been useful. For any other advice, support or to raise a concern, contact our Patient Advice and Liaison Service.

Telephone: 020 3299 3601

Email: kch-tr.palsdh@nhs.net

For information on the Health Research Authority and the Confidentiality Advisory Group visit https://www.hra.nhs.uk/.

For information on the National Data Guardian, visit https://www.gov.uk/government/organisations/national-data-guardian.

You can find out more about your information rights on the website of the Information Commissioner's Office.

To find out more about the research that is carried out, you can also read about some of our latest research.

Appendix 2 – Maternity Services Data Set information governance and fair processing guidance

This guidance document is designed to support care providers that are implementing the Maternity Services Data Set (MSDS). This guidance describes the MSDS and contains suggested fair processing information for including with existing patient information material.

This is to comply with the requirements of the common law duty of confidentiality, the Data Protection Act 2018, the General Data Protection Regulation (GDPR), NHS Constitution and the Department of Health and Social Care's Directions to NHS England, formerly known as the HSCIC, issued in 2015, 2017 and 2018 on upholding patients' national data opt out preferences.

The suggested fair processing information should not be produced as a separate information leaflet for patients and should be incorporated into existing material wherever possible.

Legal basis for the collection

NHS England has been directed by NHS England under section 254 of the Health and Social Care Act 2012 to establish and operate a system for the collection and analysis of the MSDS information:

https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/directions-and-data-provision-notices/nhs-england-directions/establishment-of-information-systems-for-nhs-services-maternity-services-directions-2015

Under GDPR, our lawful basis for processing is Article 6 (1) (c), which relates to processing necessary to comply with a legal obligation to which we are subject. Our lawful basis for processing special category data is GDPR Article 9 (2) (h) and Schedule 1, Part 1 (2) (2) (f) of the Data Protection Act 2018.

A Data Provision Notice (DPN) for the MSDS will be published to enforce the data requirements as per NHS England statutory powers, under Section 259 (1) of the Act.

Secondary use of data

NHS England has a central reporting system where an anonymised version of the MSDS will be held for reporting purposes. This platform will support the analysis of maternity services data and serve the following purposes:

- Anonymised data will be published on the NHS England website and shared with national bodies, allowing the effective monitoring of service standards, including efficiency, equity and effectiveness of service, by policy makers.

- Extracts of data will be made available to care providers and their commissioners to allow the local monitoring of service provision, assist with allocating payments and help submitters to improve data quality.

- Anonymised data will also be made available at provider level to help to inform a patient's care and treatment choices, e.g. via the NHS Choices website.

- The data held in the MSDS may also be linked to data held by NHS England from various other data sets and collections, including (but not limited to) the Community Services Data Set (CSDS) and Mental Health Services Data Set (MHSDS). The MSDS data may also be linked to external data sources such as Office for National Statistics (ONS) data and data from the National Neonatal Data Set. More information about the data sets and collections that NHS England hold and that may be used for linkage can be found on the NHS England website. Linkage is carried out in order to investigate the relationship between care in maternity services and subsequent activity, such as health visiting and school nursing activity, as well as referrals to neonatal units, mental health services and other services.

Fairness and transparency

As the MSDS data is to be used for secondary care rather than direct patient care, patients using NHS-funded maternity services must be made aware that their confidential data will be used for this beneficial, additional purpose i.e. to improve care.

Acting fairly and transparently ensures compliance with the common law duty of confidentiality, the NHS Constitution and legislation e.g. the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

Ensuring fairness is the responsibility of the care provider from which the data will be collected (NHS England has provided some suggested wording later in this document).

Patients must also be informed of their right to set a national data opt-out preference to prevent their confidential patient information from being used for purposes beyond their own direct care and treatment (e.g. for research and planning purposes). This complies with the Department of Health and Social Care's Directions, issued to NHS England in 2015, 2016 and 2018 on the upholding of patients' national data opt out preferences.

Patient choice

Providers are legally required to submit full returns of MSDS data, as the DPN that will be issued under section 259 (10) of the Health and Social Care Act 2012 sets aside the common law duty of confidence in respect of this data. However, providers may themselves exclude records where they are subject to any other restriction on disclosure e.g. by other laws.

Patients however do have a right to set a national data opt-out preference to prevent their data being used for purposes beyond their direct care and treatment. Where an opt-out is received from a patient (or their parent or guardian in the case of a child), NHS England will exclude the relevant records from any onward dissemination of the data.

Patients using these services have the right to change their minds about a disclosure decision at any time before the disclosure is made and can do so afterwards to prevent further disclosures.

Further information is available from https://digital.nhs.uk/services/national-data-opt-out-programme/guidance-for-health-and-care-staff.

Further guidance

This guidance document complies with the NHS England Code of practice on confidential information.

Fairness and transparency information for patients

A key transparency requirement under the GDPR is that individuals have the 'right to be informed' about the collection and use of their personal data. The following suggested wording is intended to be incorporated into a hospital's existing information for patients. It does not need to be a separate leaflet.

Purpose and legal basis for processing

We collect information about you (your personal data) for the Maternity Services Data Set (MSDS), to help achieve better outcomes of care for mothers, babies and children. The data set collects information about the mother's demographics (e.g. postcode, date of birth, ethnic category), booking, diagnosis and admission details, as well as details about screenings and tests and labour/delivery. The data set also collects details about the baby's demographics (e.g. date and time of birth, sex) and relevant tests prior to discharge from maternity services.

Our lawful basis for processing this data is [insert Article 6 processing condition, Article 9 processing condition and DPA 2018 schedule 1 processing condition]

What we do with it

The data is securely sent to NHS England which is the central organisation that receives the same data from all NHS-funded maternity services across England. NHS England removes all identifying details and combines the data we send with the data sent by other care providers, forming the MSDS.

The data set is used to produce anonymised reports that only show summary numbers of, for instance, patients referred to different maternity services. It is impossible to identify any individual patient in the reports, but the reports do help us to improve the care we provide to you and other patients.

No information that could reveal your identity is used in national reports.

The benefits of the MSDS to you as a patient include:

- making sure maternity services are available to all patients and measuring the respective care delivered
- better care, through monitoring progress to allow future services to enable maternity care provided is mother and child-centric
- informing patients about the care offered at different hospitals
- more personalised and better organised care for patients through understanding what care is needed nationally, for example understanding how the antenatal care provided can affect outcomes for both mother and baby

The data held in the MSDS may also be linked to data held by NHS England from various other data sets and collections, including (but not limited to) the Community Services Data Set (CSDS) and Mental Health Services Data Set (MHSDS). The MSDS data may also be linked to external data sources such as Office for National Statistics (ONS) data and data from the National Neonatal Data Set. More information about the data sets and collections that NHS England hold and that may be used for linkage can be found on the NHS England website. Linkage is carried out in order to investigate the relationship between care in maternity services and subsequent activity, such as health visiting and school nursing activity, as well as referrals to neonatal units, mental health services and other services.

For more information about how NHS England uses your personal data including their lawful basis for processing, how long they hold it for and your rights, please see their website: https://digital.nhs.uk/about-nhs-digital/our-work/keeping-patient-data-safe/gdpr/gdpr-register

To manage your choice about how your confidential patient information is used beyond your own individual care, please visit the following website https://www.nhs.uk/your-nhs-data-matters/

Alternatively, you can call 0300 303 5678.

More information about the Maternity Services Dataset (MSDS) can be found at the following website: https://digital.nhs.uk/data-and-information/data-collections-and-data-sets/data-sets/maternity-services-data-set

How long we keep it

We are required to keep your records for 25 years.

What are your rights?

You have a right to object to the processing (use) of your personal data in some circumstances by letting us know. There are legitimate reasons why we may refuse your objection, which depend on why we are processing it. This will not affect your treatment in any way.

You can also make a subject access request for information that we hold about you.

You also have the right to have inaccurate personal data rectified and to request the restriction or suppression of your personal data in specific circumstances, for example if you feel that the data held is inaccurate. Please contact us on:

Subject access request team contact details

Your right to complain

If you wish to raise a complaint concerning our handling of your personal data, please visit our Feedback and Complaints pages [insert link to your organisation’s complaints pages].

You also have a right to raise a concern with the Information Commissioner's Office at any time. Their contact details are: ICO, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF.

Appendix 3 – National Data Opt Out

National Data Opt Out

Overview

The service to apply national data opt-outs to data disclosures requires additional processing of confidential patient information (CPI). As this is classed as special category data under DPA 2018 and can involve processing data on a large scale and matching to the national opt-out data which comes from a different source we are required to inform you that this processing takes place.

The national data opt-out was introduced to give patients a choice on how their confidential patient information is used for purposes beyond their individual care. The information that the opt-out applies to is special category data as it includes information about a patient's health care and/or treatment that has been collected as part of the care we provide for the patient.

Patients can set or change their national data opt-out choice using an online or contact centre service. When a patient sets a national data opt-out it is in held in a repository on the NHS Spine against the patient's NHS number.

In accordance with the patient's wishes and national data opt-out policy, as a health and care organisation located in England, we are required to apply national data opt-outs when applicable to a use or disclosure of confidential patient information for purposes other than the patient's care or treatment.

Application of the National Data Opt Out

Applying the opt-out to a data use/disclosure requires that we check, by using the NHS numbers of patients, whether a patient has registered an opt-out before the data is used/disclosed.

To do this a separate list of the NHS numbers in the data that is going to be used/disclosed needs to be created. The list of NHS numbers is then submitted to the Check for National Data Opt-outs service via the secure Message Exchange for Social Care and Health (MESH) messaging service. The Check for National Data Opt-outs service is an external service provided by NHS England. The service checks the list of NHS Numbers against a list of opt-outs created from the repository on the NHS Spine, where a match is found it removes the NHS number from the list and then returns an updated list of NHS numbers (with opt-outs removed) back to us via MESH.

We then match the updated list of NHS numbers against our original set of data that was going to be used/disclosed and remove the entire record for those patient records where the NHS numbers match. This creates a 'cleaned' set of data with opt-outs applied that we can then use/disclose."

In order to respect and apply national data opt-outs in accordance with patient wishes it is necessary to check patient NHS numbers using the Check for National Data Opt-outs service and to process confidential patient information further in order to be able to apply national data opt-outs as described earlier. Only the minimum amount of data required i.e. the NHS number is used to check if a national data opt-out is held.

Legal Basis

The legal basis under GDPR and the Data Protection Act 2018 for us to send and receive NHS numbers (considered personal data but not special category data) to and from the Check for National Data Opt-outs service provided by NHS England is based on the following:

- **‘Personal Data**
    - 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 controller’

In addition to the Article 6 legal basis above, the legal basis under GDPR and the Data Protection Act 2018 to process confidential patient information (considered special category data) in order to apply national data opt-outs is the following:

- ‘**Special Categories of Personal Data#**
    - Article 9(2)(h) allows for processing for management of health and social care based on member state law: which is provided for in the **Data Protection Act 2018**: Schedule 1 Paragraph 2 (2)
    - Article 9(2)(f): The processing is necessary for the management of health care systems or service or social care systems or services and is processed by or under the responsibility of a health professional or a social work professional, or by another person who owes a duty of confidentiality under an enactment or rule of law’”