Sherwood Forest Hospitals
NHS Foundation Trust

Data Protection, Confidentiality and Disclosure Procedure

Document Category:	**INFORMATION GOVERNANCE**
Document Type:	**PROCEDURE**

Keywords:	Personal information, special categories of personal information, confidential information

Version:	**Issue Date:**	**Review Date:**
3	September 2023	29th September 2025

Supersedes:	Data Protection, Confidentiality and Disclosure Procedure Version 2		
Approved by (committee/group):	Information Governance Committee	**Date Approved:**	29th September 2023

Scope/ Target Audience: (delete as applicable / describe)	Trustwide

Evidence Base/ References:	NHS England, Information Commissioner's Office

Lead Division:	Corporate Services
Lead Specialty:	Information Governance
Lead Author:	Information Governance Manager
Sponsor:	Director of Corporate Affairs

	Name the documents here or record not applicable
Associated Policy	Data Protection, Confidentiality and Disclosure Policy Version 5
Associated Guideline(s)	
Associated Pathway(s)	
Associated Standard Operating Procedure(s)	
Other associated documents e.g., documentation/ forms	

Consultation Undertaken:	Information Governance Committee Information Governance Working Group

Template control:	v1.4 November 2019

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact 01623 672232 or email mailto:sfh-tr.information.governance@nhs.net

Contents

1 INTRODUCTION/ BACKGROUND

Sherwood Forest Hospitals NHS Foundation Trust (the Trust) processes a significant volume of personal and special category of data including data relating to children, vulnerable adults, employees, and other individuals for various purposes (e.g., the provision of healthcare services or for administrative purposes, such as HR and payroll). In compliance with Article 24 of the UK General Data Protection Regulation (UK GDPR) the Trust adopts internal policies and implements measures which meet the principles of data protection into the Trust.

This procedure will:

- Inform staff (including Medirest, Skanska, agency and contractor colleagues) that they are bound by a legal and common law duty of confidentiality to protect confidential information they process during the course of their work[1]. This duty is expressed in staff contracts and, for most health professionals, in their own professional codes of conduct.
- Provide guidance on keeping confidential information secure and confidential.
- Make staff aware of the correct procedures for disclosing confidential information.

Under UK GDPR, any organisation that processes personal data faces enforcement action for failing to maintain appropriate confidentiality, integrity and security. . This could also cause reputational damage.

2 AIMS/ OBJECTIVES/ PURPOSE (including Related Trust Documents)

The Trust is committed to meeting its legal obligations and NHS requirements concerning data protection and confidentiality. These obligations arise from the UK General Data Protection Regulation, Human Rights Act 1998, the Common Law Duty of Confidentiality, Caldicott Principles, and the Confidentiality: NHS Code of Practice.

This commitment is expressed in several the Trust's Information Governance objectives,

- The Trust will promote Data Protection by design and default in the way in which it processes personal data.
- The Trust will ensure patients and the public are effectively informed and know how to access their information and exercise their right of choice.
- The Trust will ensure the confidentiality of personal information.
- The Trust will ensure the security of personal information.

[1] The duty of confidentiality continues after employment with the Trust has ceased.

- The Trust will ensure that clinical and corporate information is managed in accordance with mandated and statutory requirements.

Related Trust Documents

- Data Protection, Confidentiality and Disclosure Policy Version 5.

A number of Acts and guidance dictates the need for safe haven arrangements to be set in place, they include:

UK General Data Protection Regulation (Principle f): You must ensure that you have appropriate security measures in place to protect the personal data you hold.

This is the 'integrity and confidentiality' principle of the GDPR – also known as the security principle.

Code of Practice on Confidential Information[2]:
"Care must be taken, particularly with confidential clinical information, to ensure that the means of transferring from one location to another are secure as they can be".

The Caldicott Guardian Manual[3] – the Caldicott Guardian should oversee all arrangements, protocols and procedures where confidential patient information may be shared with external bodies both within, and outside, the NHS. This includes flows of information to and from partner agencies, sharing through the NHS Care Records Service (NHS CRS) and related IT Systems, disclosure to research interests and disclosure to the police.

Information Security Management: NHS Code of Practice[4] – all individuals who work within, or under contract to, an NHS organisation have a general responsibility for the security of information that they create or use in the performance of their duties.

NHS Information Governance – Guidance on Legal and Professional Obligations[5] – this document lists the relevant legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed.

[2] https://digital.nhs.uk/binaries/content/assets/legacy/pdf/8/9/copconfidentialinformation.pdf
[3] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/581213/cgmanual.pdf
[4] https://digital.nhs.uk/binaries/content/assets/legacy/pdf/8/9/copconfidentialinformation.pdf
[5] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200702/NHS_Information_Governance_Guidance_on_Legal_and_Professional_Obligations.pdf

3 ROLES AND RESPONSIBILITIES

Committees

Trust Board
The Trust Board is ultimately responsible for Information Governance within the organisation and is also responsible for ensuring that sufficient resources are provided to support the requirements of the procedure.

Information Governance Committee
The Committee is responsible for ensuring that this policy is effectively implemented, including any supporting guidance and training deemed necessary to support the implementation, and for monitoring and providing Board assurance in this respect.

Chief Executive
The Chief Executive has overall responsibility for this procedure within the Trust. Implementation of, and compliance with this policy is delegated to the Senior Information Risk Owner, Caldicott Guardian, Data Protection Officer, and members of the Information Governance Committee.

Senior Information Risk Owner
The Director of Corporate Affairs is responsible to the Chief Executive for Information Governance and is the designated Senior Information Risk Owner, who takes ownership of the Trust's information risk policy, acts as an advocate for information risk on the Board and provides written advice to the Chief Executive on the content of the Statement of Internal Control in regard to information risk. The Senior Information Risk Owner also reports annually to the Trust Board on Information Governance performance.

Caldicott Guardian
The Medical Director is the 'conscience' of the organisation, providing a focal point for patient confidentiality, information sharing and advising on the options for lawful and ethical processing of information as required.

Data Protection Officer
We are a public authority and have appointed a Data Protection Officer. The Data Protection Officer reports to the Senior Information Risk Owner and works with the Caldicott Guardian. The Data Protection Officer is tasked with monitoring compliance with Data Protection legislation, our data protection policies, awareness-raising, training, and audits. Our Data Protection Officer acts as a contact point for the Information Commissioner's Office. When performing their tasks, our Data Protection Officer has due regard to the risk associated with processing operations, and considers the nature, scope, context and purposes of processing.

Information Asset Owners (IAOs)
Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the relevant business. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result, they are able to understand and address risks to the information and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

Information Asset Administrators (IAAs)
Information Asset Administrators ensure that Information Governance policies and procedures are followed, recognise actual or potential Information Governance security incidents and take steps to mitigate those risks, consult their Information Asset Owners on incident management, and ensure that information asset registers are accurate and up to date. When carrying out a Data Protection Impact Assessment, we seek the advice of our Data Protection Officer who also monitors the process.

Directors and Services Managers
Responsible for ensuring a comprehensive risk assessment is undertaken for evaluation and approval by the Information Governance Committee, also ensure that risk assessments are accurately maintained, and risks re-evaluated and updated if significant changes are made to services. (See 6.16)

Duty Nurse Managers
Out-of-hours or on occasions when the Caldicott Guardian, Information Governance Manager or Information Asset Owner are unavailable, Duty Nurse Managers in the first instance will be required to assume responsibility for any decision regarding urgent disclosures that cannot be delayed, they can if necessary, seek assistance from staff involved in the Gold/Silver On-Call Protocol consulting with the Trust's Legal Advisors as necessary.

All Staff
All staff (including Medirest, Skanska, agency and contractor colleagues)who use and have access to Trust personal information must understand their responsibilities for data protection and confidentiality.

Contractors and agency staff and other third parties' staff are under instructions to report all incidents, their causes and resolving actions to their own line managers. The Trust reserves the right to audit the supplier's contractual responsibilities or to have those audits carried out by a third party.

The Trust will expect an escalation process for problem resolution relating to any breaches of Information Governance security and/or confidentiality of personal information by the Contractor's employee and/or any agents and/or sub-contractors.

Any Information Governance security breaches made by the Contractor's employees, agents or sub-contractors will immediately be reported to the Trust's Information Governance Team sfh-tr.information.governance@nhs.net.

Third parties contracting services to the Trust must sign a confidentiality agreement, countersigned by the Information Asset Owner. This ensures that their employees undertake annual data security awareness training, have read and understood our data protection and confidentiality policy and accept their personal responsibility to maintain confidentiality at all times.

Managers or health professionals who are responsible for any seconded / work experience placement should ensure that all students have read and understood our data protection and confidentiality policy and accept their personal responsibility to always maintain confidentiality.

4	**PROCEDURE DETAILS (including Flowcharts)**

4.1 CALDICOTT PRINCIPLES

1. **Principle 1 - Justify the purpose for using confidential information.**

This means you should not use or share information unless you have a valid reason.

For example, wanting to send a friend a birthday card is not a valid reason to access the records your organisation holds about them.

2. **Principle 2 – Do not use the confidential information unless it is absolutely necessary.**

If you believe you have a valid reason, ask yourself if it is essential that you use confidential information, or can the purpose be met without identifying any individual?

For example, if you are asked for information about how many people have attended for an appointment, it would not be necessary to provide the names and addresses of each person who attended.

3. **Principle 3 - Use the minimum necessary confidential information.**

If you must use confidential information, you need to be clear on what is required to meet the purpose. If a particular part of the information is not necessary, it should not be used or shared.

For example, if you receive a valid request for details about a patient/service user's last attendance at your organisation, it would not be appropriate to provide the requestor with the entire record or care/treatment.

4. **Principle 4 - Access to confidential information should be on a strict need-to-know basis.**

Information should only be available to authorised members of staff. You should not attempt to access information that you do not need to see as part of your role or use someone else's account details.

You should never allow anyone to log into systems using your details. If you intend to share the information, it should only be shared with those who need it to conduct their role.

5. **Principle 5 - Everyone with access to confidential information should be aware of their responsibilities.**

You should attend the provided training and awareness session so that you understand your responsibilities for protecting information.
If you intend to share the information, you must ensure that the recipient is aware of their responsibility for protecting the information and of the restrictions on sharing it further.

6. **Principle 6 - Understand and comply with the law.**

When you use confidential information, there is a range of legal obligations for you to consider. The key obligations are outlined in the Common Law Duty of Confidentiality and under the Data Protection Act.

If you have a query about the disclosure of confidential information, you should contact your line manager, then the Information Governance lead (or equivalent) if you are still not sure.

7. **Principle 7 - The duty to share information can be as important as the duty to protect confidentiality.**

You should have the confidence to share information in the best interests of your patients and service users within the framework set out by these principles.

8. **Principle 8: Inform patients and service users about how their confidential information is used.**

A range of steps should be taken to ensure no surprises for patients and service users, so they can have clear expectations about how and why their confidential information is used, and what choices they have about this. These steps will vary depending on the use: as a minimum, this should include providing accessible, relevant, and appropriate information - in some cases, greater engagement will be required.

4.2 USE OF CONFIDENTIAL PATIENT INFORMATION FOR PURPOSES BEYOND INDIVIDUAL CARE

Use of confidential patient information for non-healthcare purposes[6] typically falls into two categories:

I. Research – usually conducted with explicit patient consent or approved (under section 251 of the National Health Service Act 2006) by the Health Research Authority
II. Planning – activities to evaluate and improve services.

However, this use of confidential patient information must comply with data protection legislation, common law duty of confidentiality and the Caldicott principles.

4.2.1 Research

Our Trust is a research active organisation that encourages a research positive culture to give patients wider access to clinical research and improve patient care and treatment options. During a visit, patient's' may be approached by a member of the Clinical Research team informing them of possible clinical trial opportunities.

Consent is an important part of the research process and is frequently sought for participation in research studies. In most instances we will rely on Article 6 (1)e and Article 9 (2)j of the UK GDPR if and when we use patient information for research. If patients have formally consented to take part in research, this will satisfy the common law duty of confidentiality and they will be informed how information about them will be used. Where it has been impracticable to obtain consent, we will seek approval from the Secretary of State via the Confidentiality Advisory Group under Section 251 of the National Health Service Act 2006. For further information on this legislation please visit the Government's UK legislation Website.

Patients have a choice about whether they want their confidential information to be used in this way. If they happy with this use of information they are not required to do anything. If they do choose to opt-out confidential patient information will still be used to support individual care. please visit www.nhs.uk/your-nhs-data-matters.

The guidance below outlines the relevant time frame patient records should be retained if they have participated in a clinical trial.

The rationale for retaining patient records for an appropriate period is to allow further analysis and safety monitoring by regulatory authorities as necessary.

The Medical Research Council (MRC) has set out guidance for the time frame of the retention of medical notes below:

[6] Healthcare purposes include all activities that directly contribute to the diagnosis, care, and treatment of an individual and the audit/assurance of the quality of healthcare provided. They do not include research, teaching, financial, audit, or other management activities.

- For basic research –research data and data material should be retained for 5 years after the completion of the trial.
- For population health and clinical studies, the records and research data should be retained for 20 years after the study has been completed.
- Studies that require records to be retained for more than 20 years must have a valid justification.
- In some cases, the sponsor of the clinical trial may have set guidance for a specific retention time which differs from the MRC. In such cases the sponsor guidance should be followed.

In order to identify patient records that must be retained in this way a yellow alert sticker is placed on the red alert page in the inside of a patients' notes.
If there is any doubt or concern over how long an individual patient's record should be stored, please contact the Head of Research and Innovation.
Here is a link to their Privacy Notice.

The use of patient identifiable information for research usually requires explicit patient consent. It is also important that only staffs who are members of the direct care team recruit patients to studies or introduce patients to research staff.

When seeking consent for disclosure, staff must ensure that patients are given enough information to allow them to make a considered and informed decision. Specifically, he/she should be informed of the reasons for the disclosure, the way that it will be made and the possible consequences. The exact amount of disclosure and the identity of those who will receive it should also be explained.

If a patient cannot be contacted to give consent, it should not be assumed that their medical details cannot be used for research purposes.

4.2.2 PLANNING

Data can only be used for purposes beyond individual care and treatment in specific circumstances. There must be a legal basis for any disclosure of data, and the use must benefit health and care.

Planning uses may include:

- understanding what care and treatment patients need
- predicting what services will be needed in the future, so funding and resources can be put into place.
- understanding the outcomes of patient care to make sure patients are being cared for safely and effectively.

Sometimes we work in partnership with commercial organisations to plan and provide services. For example, health and care analysis companies can be employed by NHS trusts and care organisations to measure effectiveness and identify improvements. The Trust will provide the data and has all legal responsibility for it and will put a contract in place to cover the data sharing arrangements. Read more information about companies using health information.

The national data opt-out covers use and disclosure of confidential patient information for research and planning. If you are planning on disclosing data to another organisation, you will need to comply with the policy. You also need to comply if you are changing the way you use confidential patient information, to use it for research and planning internally, when it was previously only used for individual care and treatment.

The **National Data Opt-Out** allows a patient to choose if they do not want their confidential patient information to be used for purposes beyond their individual care and treatment - for research and planning. Patients, or people acting for them by proxy, have control over setting or changing their own opt-out choice, and can change their mind at any time. In most cases health and care staff won't be involved - but it's helpful to understand how the process works so you can tell patients where to find out more about their choices. When a patient sets an opt-out choice, it is recorded against their NHS number on the Spine. It will remain unless the patient changes their mind, even after they have died. If a patient has agreed to a specific use of data, after being fully informed, then the national data opt-out does not apply. Even patients who have registered a national data opt-out can agree to take part in a specific research project or clinical trial, by giving their explicit consent. Our National Data-Opt-Out procedure is available here[7]. Details of how a patient can register their wishes is available here[8].

In certain cases, it has been agreed that the National Data Opt-Out should not be applied to programmes which have section 251 approval. More information and a list of the programmes for which the NDDO should not be applied to is available. This list is subject to change so please ensure you check the most up to date version. The organisation requesting the data can also inform you that the National Data Opt-Out does not apply.

Where an audit is to be undertaken by the clinical team that provided care, or those working to support them (such as clinical audit staff), confidential information may be used assuming implied consent provided that patients have been informed that their data may be used for this purpose and have not objected[9].

[7] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=12805
[8] https://www.nhs.uk/your-nhs-data-matters/
[9] If a patient does object you should explain why the information is needed and how this may benefit their own, and others' care. If it is not possible to provide safe care without disclosing information for audit, you should explain this to the patient and the options open to them. (General Medical Council: Confidentiality Guidance, Protecting and Providing Information. 2009)

4.3 DISCLOSURES

Police requests

1. All requests from the Police for information about patients should be forwarded to the Information Governance team sfh-tr.sar@nhs.net during normal working hours i.e., Monday to Friday between 09:00 and 17:00. Out of normal working hours requests may be dealt with by the Duty Nurse Manager, liaising with Gold/Silver as necessary but ensuring that the Information Governance team are copied into all correspondence with the Police sfh-tr.sar@nhs.net.

2. Requests from the police for information about staff should be forwarded to the Information Governance team sfh-tr.sar@nhs.net during normal working hours i.e., Monday to Friday between 09:00 and 17:00. Information Governance will liaise with the relevant HR Manager.

3. Common requests relate to the prevention, detection, investigation and punishment of serious crime and/or to prevent abuse or serious harm to others. Examples include murder, rape, child protection concerns, serious assault.

4. Police information enquires relating to information disclosure ordinarily fit into one of the following categories:

A. **ROUTINE** formal requests for patient information in relation to prevention or detection of crime (dealt with via a formal Request Form Procedure - see section 4.4).
B. **URGENT** requests to establish the whereabouts or condition of an individual where the subject's safety or wellbeing is urgently in question. (For Procedure see section 4.5).

5. Where a records disclosure in response to such an application is legally justifiable, original copies of records will normally be retained by the Trust and relevant scanned copies of records will be supplied to a secure pnn email address. This action ensures that only relevant information is disclosed and that original records remain available to the Trust for NHS purposes and that the continued integrity of an original record is maintained.

6. There are very few special circumstances in which original health records can be removed from Trust premises in order to satisfy a request for disclosure these are:

- To comply with some specifically worded legal orders.
- At the request of HM Coroner (usually via the Police)
- In accordance with Section 19-21, Police and Criminal Evidence Act 1984 in which a police officer may seize a record as evidence when investigating a case involving the Trust or its employees.

7. In all these circumstances the Information Governance team must take and retain a copy of the original record before it leaves the Trust's premises, in order that the Trust retains its own copy for reference. In all cases the records must be tracked on the records

tracking system to the destination to which they have been taken, a contact telephone number recorded and a signed receipt for the record should be obtained and retained by the Information Governance team.

8. Records that may be required as evidence – The police will advise if an original record is likely to be required in connection with legal proceedings at a future time and will attach an evidence tag. Any such records will be retained by the Information Governance team until after legal proceedings have taken place.

Solicitors' requests

9. Solicitors usually act on behalf of individuals when they approach us for information. Requests for information in relation to a claim against the Trust should be forwarded to Legal Services sfh-tr.Legal@nhs.net.

Court orders

10. Court orders are issued by a Judge or Magistrate to compel release of copies of information. Court Orders are sometimes directed to a member of staff as an officer of the Trust (e.g., Chief Executive, Trust Secretary etc) or addressed to the organisation. Court orders will generally request very specific documents or information and should be forwarded to the Information Governance team sfh-tr.sar@nhs.net.

11. Court Orders must be treated with the highest priority. It is a criminal offence ('contempt of court') to disobey a Court Order without justification ('contempt of court'). The Trust endeavours to comply with all deadlines and legal exemptions set out in the Orders for disclosure of information to courts.

12. Legal orders have a strict timescale attached to them and it is important that staff do not put them into the general internal post system or delay them in any way. These should be hand delivered to the Information Governance team.

13. Information Governance team will notify the Information Governance Manager of all Court Orders received, and a monitoring system will be operated to ensure all timescales for disclosure are met.

14. Where Courts have made an Order, the required information must be disclosed, unless the organisation decides to challenge the order at court. Where sensitive information is contained that is not relevant to the case, the Trust may raise ethical and Data Protection i.e., data minimisation concerns by contacting the judge or presiding officer to advise that the order be amended.

HM Coroner

15. The Coroner's Office may request a medical record in order to investigate the cause of death of a person in suspicious or unnatural deaths. Information may be requested by a police officer on behalf of HM Coroner. The police officer must provide a letter detailing the request from the coroner and signed by the coroner. A receipt must be taken when

records are collected and retained by the Mortuary. All requests must be sent to sfh-tr.sar@nhs.net or hand delivered to the Information Governance team.

Requests about children, young people or vulnerable adults

16. Any requests for information about children or vulnerable adults, where there are safeguarding issues highlighted within the record, should be forwarded to the relevant Safeguarding Team for review (adult's sfh-tr.safeguardingadults@nhs.net, children sfh-tr.safeguardingchildren@nhs.net) via the Information Governance team.

17. The Trust has named Doctors trained in issues relating to both Safeguarding Children and Adults. They can be contacted for advice via switchboard. The Trust has an information sharing agreement in place with other public authorities including the Police.

i. Child Sexual Abuse (CSA):

18. After examinations a medical report is produced, and this report is automatically provided to the police in addition to the GP and Social Care. Consent is always explained to the young person and family involved and they are informed at the time that a report will go to the Police and may be used in Court.

19. Faxed requests for Child Sexual Abuse (CSA) Medical Reports will no longer be accepted and requests should be sent to sfh-tr.sar@nhs.net to be dealt with by the Information Governance team in liaison with the relevant Safeguarding Team. Police requesting information must be clear whether it is a Child Sexual Abuse report or a copy of medical records they are requesting. Request for photocopies of health records will be processed via normal Routine procedures (see Appendix C).

ii) Non-Accidental Injury (NAI) Reports:

20. Police are requested to email requests for copy non-accidental injury reports to sfh-tr.sar@nhs.net. A copy of the information will be sent to a secure pnn email address. Supporting documentation of all requests received will be maintained as a record by the Information Governance team.

Documentation will consist of:

- The original written and signed police request.
- The date and time of receipt of request
- Record of the specific documents disclosed.
- Receipt signed by the police officer on collection, date and time recorded.

21. When a non-accidental injury report is carried out or photographs taken either at the Trust's premises or by Trust Clinical staff in the community, these records will be routinely filed within the patients' medical record behind a safeguarding divider. If a Trust medical record does not exist, then the patient will be registered on Medway PAS by the Information Governance team, and one created.

22. Request for copies of health records will be processed via normal routine procedures completing the application in Appendix B).

Disclosures to support external investigations.

23. NHS Protect, the Coroner's Office and professional regulatory bodies, such as the General Medical Council and Nursing and Midwifery Council, may compel staff to provide personal and confidential information to support an investigation.

24. However, staff should seek advice from Information Governance to ensure that any information requests are processed by the Information Governance team in order to ensure information disclosed is appropriate and not excessive.

25. Consultants may provide a professional opinion in relation to other external investigations. However, all other staff should not provide witness statements without first consulting Information Governance and Legal Services.

Disclosures to Department of Work and Pensions

26. There are three elements of disclosures relating to the Department of Work and Pensions or their representatives:

1. Confirmation of attendance of Out-patient Appointment/IP Admission
2. Request for a Medical Report from a Clinician
3. Request for copies of Health Records.

All requests to the Trust are processed by the Information Governance team and require consent from the individual. Responses will be provided within 10 working days.

Disclosures to Health Insurance Companies

27. Disclosures relating to confirmation of patient hospital attendance are completed by the Information Governance team at the patient's own request.

Disclosures from Close Circuit Televisions (CCTV)

28. The Trust has notified the Information Commissioner of the Trust's CCTV data processing activity for the purposes of crime prevention including aggressive/abusive behaviour and the detection, apprehension, and prosecution of offenders.

29. The Trust's CCTV schemes operate in accordance with the Protection of Freedoms Act set out in the picture: A data protection code of practice for surveillance cameras and personal information.[10]

30. The Information Governance team will process requests for disclosure of (CCTV) films to the police where:

- Powers under the Police and Criminal Evidence Act 1984 have been invoked and an appropriate written application made under the Data Protection legislation applies.
- There is a Court Order.

[10] https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

Pathology Disclosures

31. The Pathology Service receives and manages requests directly for pathological specimens required in connection with police and legal proceedings and have Standard Operating Procedures for dealing with such requests.

32. Tissue samples from the deceased are regulated under the Human Tissue Act. Consent is required from a person in an appropriate qualifying relationship (see separate Consent to post-mortem examination policy) or a court order. Any samples removed from the department must comply with Human Tissue Authority requirements for record keeping and documentation.

33. Tissues from the living require appropriate consent or court authority before being released.

34. Requests should be addressed to the Head of Pathology Services who will cascade them appropriately. All individuals across the Trust should be aware of this procedure and in conjunction with the Data Protection, Confidentiality and Disclosure Policy, as part of their own accountability for Information Governance.

Disclosures under the Road Traffic Act 1998

35. If a patient has been involved in a road traffic accident, the Trust is obliged under the Road Traffic Act and the Police Reform Act to give police information which will lead to the identification of the driver and passengers (no other information is required).

36. Disclosures of person identifiable information are usually only made with the understanding and agreement of the individual. In certain circumstances, an NHS Body or member of staff may have a statutory duty to pass on person identifiable information, a list is provided below but is not exhaustive:
    - Accidents - Health and Safety at Work Act.
    - Addiction - Misuse of Drugs Notification and Supply to Addicts 1985
    - Births and Deaths - Notification of Births and Deaths Regulations 1974
    - Driver of a vehicle - Road Traffic Act 1972
    - Infectious Diseases - Public Health (Infectious Diseases) Regulation 1988
    - Subpoena - Police and Criminal Evidence Act 1984
    - Suspicious deaths - Coroner
    - Termination of Pregnancy - Abortion Act 1967
    - Terrorism - Prevention of Terrorism Act 1989

The Trust is also required to disclose information to other agencies to promote cooperation and the sharing of information for the provision of ongoing care, for example:

- Criminal Injuries
- Industrial Inquiries Benefits
- Pensions
- Social Services
- Welfare rights

In addition to the requirements of the above-named Acts, the Trust recognises that it has a duty to cooperate with the Police and their official enquiries. If you are in any doubt regarding any of the above, please seek advice from the Information Governance Team.

Protecting confidentiality and privacy on the telephone

37. We encourage the use of telephone communications with patients and service users to support the delivery of care. When making or receiving telephone calls, for example, to set up an appointment, you need to follow simple safety precautions to ensure the privacy of the person you are calling. You should:

- Double check the number before dialling.
- Check your location: make sure that your telephone conversation cannot be overheard.
- When your call is answered: give your full name, **without specifics about the service or purpose of the call**. Ask to speak to the relevant person by their full name.
- When the relevant person answers or comes to the phone, verify the person's identity: check the identity of the person you are speaking to by asking for two or three details such as their date of birth, postcode, and the first line of their address.
- Once you are satisfied you are speaking to the right person, tell them the service you are calling from and the purpose of the call.
- When someone else answers the phone: give your full name, but not the service or purpose of the call. Ask if there is a better time to speak with the person and end the call, even if the recipient applies pressure to extend it. Try calling again at the suggested time if possible.
- In case the call goes to voicemail: leave the patients full name, your full name and that you are calling from Sherwood Forest Hospitals NHS Foundation Trust with our contact telephone number 01623 622515.

Patients have a right to privacy so we must respect their wishes about what information is shared and to whom whether this is over the phone, in person or by letter.

Where it is justified, information may be given if certain precautions are taken. These include:

- A justified reason to speak to someone on their behalf, e.g., it is in their best interests.
- Ensuring that procedures are carried out to confirm/verify the identity of the caller, e.g., verifying the information we have about the patient (i.e., Dob, address, etc.) and that it is appropriate that they receive the information being asked for ie do you have patient consent?
- Any concerns that a caller may not be who they say they are, or that they are asking for information that they are not entitled to must be escalated to your line manager and, if necessary, the Information Governance Team. Under these circumstances no information should be disclosed
- Taking a phone number that can be checked against records and phoning back from a location where the conversation cannot be overheard.

4.4 ROUTINE POLICE INFORMATION REQUESTS – FORMAL REQUEST PROCEDURE

1. In office hours (Mon-Fri, 9am-5pm) all police enquiries concerning the disclosure of patient records/recorded information where patient consent cannot be provided, must be made in writing and sent by email or post to:

Access to Health Records
King's Mill Hospital
Mansfield Road
Sutton in Ashfield
Nottinghamshire
NG17 4JL

Tel: 01623 622515 ext. 3233
Email: sfh-tr.sar@nhs.net

Out of hours and during Bank Holidays all routine requests should be emailed to the above office for attention when the office re-opens.

2. **Formal Request Forms**

Police forces use a standard form for applying for recorded information designed in association with the Information Commissioner and the Association of Chief Police Officers (ACPO).

3. To be accepted for consideration by the Trust a completed request form must be submitted and:

- Sufficiently detail the crime being investigated.
- Be clear about specifically what information is being requested.
- Set out the reason for the enquiry (i.e., the appropriate DPA exemption)
- Detail how absence of this information would be likely to prejudice the enquiry.
- Be correctly dated and authorised by an officer above the rank of Sergeant whose status, name, badge number and station where based is confirmed.

Failure to meet these criteria could mean that the Trust and the requesting officer or both are committing a criminal offence. The requesting and authorising officers are each making a statement that the conditions given are true. Further advice on disclosures to the Police are available in the Confidentiality NHS Code of Practice.[11]

4. **Requests accompanied by patient consent.**

Where it is possible to gain patient consent it should always be requested by the police and provided with the written request if it is reasonable to do so. However, there are some

11 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf

instances where this is not possible or appropriate as it may be detrimental to an enquiry or investigation.

5. Requests without patient consent

5.1 Where consent cannot be obtained police forces use the standard request form referenced above and set out within the form the circumstances of the enquiry (see above).

5.2 The UK General Data Protection Regulation allows the release of personal information to the police for the prevention or detection of crime or the apprehension and prosecution of offenders. The data may relate to suspects, offenders or witnesses. This exemption is not a blanket exemption – it can only be claimed on a case-by-case basis. Please note as an employee we should not feel pressured to release information. All requests should be forwarded to the Information Governance team for review and release if appropriate.

5.3 For a disclosure to be made there must be a justifiable reason which is deemed appropriate under the UK General Data Protection Regulation or other legislation (See Section 6 on Legislation) and authorised by one of the following staff:

- Caldicott Guardian
- Chief Financial Officer (Senior Information Risk Owner)
- Information Governance Manager and Data Protection Officer
- Patient Services Manager
- Emergency Department Consultants
- Silver/Gold Command
- Director of Corporate Affairs
- Named Doctor/Nurse Safeguarding Children.

5.4 Any member of staff making an information disclosure to the police without accompanying patient consent must make a record of circumstances, so that there is clear evidence of the reasoning used and the circumstances prevailing. The police request forms act as a record to the Trust if and when information is disclosed, completed documentation should be sent to Access to Health Records team where records will be centrally retained for 10 years. It may be necessary to justify such disclosures to the courts or to regulatory bodies and a clear record of the decision-making process and the advice sought is in the interest of both staff and the Trust.

5.5 If necessary, and after seeking appropriate legal advice via the Information Governance team, the reviewing member of staff can refuse a request and ask the police for a Court Order.

4.5 URGENT POLICE INFORMATION REQUESTS – FORMAL REQUEST PROCEDURE

1. The police are able to telephone URGENT REQUESTS ONLY (strictly restricted to calls establish the whereabouts of an individual where the subject's safety or well-being is urgently in question) to the Ward Leader, Emergency Department. All other enquires must follow the Routine Requests – Formal Request Procedure.

2. Officers will state who they are, give a contact number which will be 0300 300 999 plus extension /department number (NOT Direct Dial number).

3. The exact purpose of the request will be stated e.g., for a vulnerable missing person, person believed collapsed in house etc and that the information is required for a 'policing purpose' to ensure safety, preservation of life or the vital interests of the data subject.

4. A VISION (Police terminology) Message reference number will be given for refer back purposes.

5. The urgency of refer back will be intimated i.e that officers are waiting to secure entry to a building or that the request is part of a routine Missing from Home enquiry and therefore not as urgent. A refer back time period will be agreed over the phone.

6. Ward Leader in Charge will give their own name and contact details to the enquiring officer for future refer back purposes.

7. Ward Leader in Charge will consider the request for information and refer to the Duty Nurse Manager if they feel any doubt as to the appropriateness of the disclosure.

8. Ward Leader in Charge/the Duty Nurse Manager will telephone back to the police officer via a contact number which will be 0300 300 999 plus extension /department number (NOT Direct Dial number) to verify the identity of the caller before making any verbal disclosure of information.

4.6 CHECKLIST FOR EMERGENCY DISCLOSURE OF PERSONAL INFORMATION TO THE POLICE

1. Identity confirmation

Is the person who they say they are? Good practice is to ask for name and rank and return the call via switchboard or office number, not mobile or direct dial.

2. UK General Data Protection Regulation Exemption

Confirm that the person asking for the information is doing so to prevent or detect a crime or prosecute an offender.

3. Emergency Request

Confirm this is an emergency request, i.e., a life-or-death situation, or where immediate legal proceedings are underway, or if the details were not provided almost immediately it would significantly harm any individual.

4. Serious Crime or Road Traffic Accident Investigation

Confirm that the alleged crime is 'serious' and carries a prison sentence of 5 years or more to justify breach of confidence. Alternatively, confirm that the patient has consented to release of their personal information.

5. Justification

Will this personal information assist attempts to prevent crime or catch a suspect?
Is it necessary to provide this information or can it feasibly be found from another source?

6. Proportionality

Is only the minimum information required being released? All releases of information to the Police should be formally logged by the access to records team sfh-tr.sar@nhs.net.

4.7 RIGHTS OF INDIVIDUALS

Access to medical records

Requests for access to medical records are centrally managed by the Information Governance Team within the provisions of data protection legislation. All appropriate documents and guidance notes on how to make a Subject Access Request are available from the general office at Kings Mill hospital and Newark hospital and published on the Trust's website[12].

A copy of the patient's medical record must be released to them within one month, subject to receipt of an adequate verbal or written request. We calculate the time limit from the day after we receive the request (whether the day after is a working day or not) until the corresponding calendar date in the next month e.g., we receive a request on 3 September. The time limit will start from the next day (4 September). This gives us until 4 October to comply with the request. If this is not possible because the following month is shorter (and there is no corresponding calendar date), the date for response is the last day of the following month. If the corresponding date falls on a weekend or a public holiday, we have until the next working day to respond.

This means that the exact number of days we must comply with a request varies; depending on the month in which the request was made e.g., we receive a request on 30 March. The time limit starts from the next day (31 March). As there is no equivalent date in April, the organisation has until 30 April to comply with the request. If 30 April falls on a weekend, or is a public holiday, we have until the end of the next working day to comply.

The Trust can refuse to comply with a subject access request if:

- The individual requesting the information has not provided enough supporting information in order for the **information to be located or their identity verified**[13]. If we have doubts about the identity of the person making the request, we can ask for more information. However, we will only request information that is necessary to confirm who they are. The key to this is proportionality. We will let the individual know as soon as possible that we need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when we receive the additional information.

- **Manifestly unfounded**:
  - the individual clearly has no intention to exercise their right of access. For example, an individual makes a request, but then offers to withdraw it in return for some form of benefit from the organisation; or

[12] https://www.sfh-tr.nhs.uk/our-services/access-to-health-records/

[13] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/#12

- the request is malicious in intent and is being used to harass an organisation with no real purpose other than to cause disruption. For example, the individual explicitly states, in the request itself or in other communications, that they intend to cause disruption.
- makes unsubstantiated accusations against you or specific employees which are clearly prompted by malice.
- targets a particular employee against whom they have some personal grudge; or
- systematically sends different requests to you as part of a campaign, e.g once a week, with the intention of causing disruption.

- Manifestly excessive:
- To determine whether a request is manifestly excessive we need to consider whether it is clearly or obviously unreasonable. We will base this on whether the request is proportionate when balanced with the burden or costs involved in dealing with the request. This will mean considering all the circumstances of the request, including:

- the nature of the requested information.
- the context of the request, and the relationship between you and the individual.
- whether a refusal to provide the information or even acknowledge if you hold it may cause substantive damage to the individual.
- your available resources.
- whether the request repeats previous requests, and a reasonable interval has not elapsed; or
- whether it overlaps with other requests (although if it relates to a separate set of information, it is unlikely to be excessive).

In either case we will justify our decision. We will base the reasonable fee on the administrative costs of complying with the request. If we decide to charge a fee, we will contact the individual promptly and inform them. We do not need to comply with the request until we have received the fee.

In determining whether it is reasonable to disclose the information, we consider all the relevant circumstances, including:

- the type of information that we would disclose.
- any duty of confidentiality we owe to the other individual.
- any steps we have taken to seek consent from the other individual.
- whether the other individual can give consent; and
- any express refusal of consent by the other individual

A patient requesting access to their medical records may be refused access to parts of the information if an appropriate clinician deems exposure to that information could cause physical or mental harm to the patient. Clinicians should be prepared to justify their reasons in a court of law if necessary. In all cases reasons for non-disclosure should be documented.

If a patient or their representative is unhappy with the outcome of their access request, e.g., information is withheld from them, or they feel their information has been recorded incorrectly within their health record, the patient or their representative can:

- request to have inaccurate personal data rectified, or completed if it is incomplete.
- meet the lead health professional to resolve the complaint.

- utilise the Trust's Complaints procedure[14]
- take their complaint direct to the Information Commissioner[15]

Staff access to their personnel record

Employee personal information and the rights of access to information are the same as for patients. All information held in a member of staff's personnel file is confidential and must be kept securely. However, the Trust supports a 'no surprises' culture and managers should offer their staff reasonable access to their own personnel files.

If staff are unhappy with the outcome of their subject access request, e.g., information is withheld from them, or they feel their information has been recorded incorrectly they or their representative can:

- request to have inaccurate personal data rectified, or completed if it is incomplete.
- utilise the Trust's Complaints procedure[16]
- take their complaint direct to the Information Commissioner[17]

Managers must bear in mind that staff are entitled to access all information the Trust holds about them, and this information should be disclosed unless there are lawful grounds for withholding it.

Information given in confidence about a member of staff may not offer grounds for withholding that information, although it may be possible to redact information to respect the privacy of third parties.

[14] https://www.sfh-tr.nhs.uk/about-us/contact-us/advice-and-support/make-a-complaint/

[15] https://ico.org.uk/make-a-complaint/

[16] https://www.sfh-tr.nhs.uk/about-us/contact-us/advice-and-support/make-a-complaint/

[17] https://ico.org.uk/make-a-complaint/

5 EDUCATION AND TRAINING

TRAINING

Annual data security awareness level 1 (formally known as Information Governance) training is mandatory for all new starters as part of the induction process. In addition, all existing staff must undertake data security awareness level 1 training on an annual basis. Staff can undertake this either face-to-face[18] or online. Provision is available online (or face to face for staff who do not have routine access to personal data) and includes Data Protection and confidentiality issues.

Data security awareness level 1 session meets the statutory and mandatory training requirements and learning outcomes for Information Governance in the UK Core Skills Training Framework (UK CSTF) as updated in May 2018 to include General Data Protection Regulations (GDPR).

Our Senior Information Risk Owner, Information Asset Owners and Information Asset Administrators must attend regular information risk awareness training which is available from the Information Governance team.

IMPLEMENTATION

A copy of this policy and all related policies and procedures are provided to all staff and patients on the Trust's website.[19]

COMMUNICATION

As part of induction all new staff will be made aware of the location of all policies and procedures. This procedure will be available on the Trust's website. Any changes to the procedure will be communicated to staff via the weekly staff bulletin and additional information and training provided for managers as required.

[18] https://sfhcoursebooking.nnotts.nhs.uk/default.aspx (internal web link)
[19] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/

6 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum requirement to be monitored	Responsible individual/ group/ committee	Process for monitoring e.g., audit	Frequency of monitoring	Responsible individual/ group/ committee for review of results	Responsible individual/ group/ committee for development of action plan	Responsible individual/ group/ committee for monitoring of action plan
Review of inventory of corporate records	Information Governance Manager	Review	Annually	Information Governance Team	Information Governance Team	Information Governance Committee
Adherence to UK GDPR, Freedom of Information Act, and other relevant legislation	Information Governance Manager	Monitor	Annually	Information Governance Team	Information Governance Manager	Audit & Assurance Committee

The Trust will regularly monitor its safe haven practices for compliance with this procedure.

Local areas and services will audit their own practices from time to time, at least annually to measure compliance with this procedure or in light of future requirements.

7 EQUALITY IMPACT ASSESSMENT (please complete all sections)

Name of procedure being reviewed: Data Protection, Confidentiality and Disclosure Procedure			
New or existing procedure: Existing			
Date of Assessment: 6th July 2021			
For the service/policy/procedure and its implementation answer the questions a – c below against each characteristic (if relevant consider breaking the policy or implementation down into areas)			
Protected Characteristic	a) Using data and supporting information, what issues, needs or barriers could the protected characteristic groups' experience? For example, are there any known health inequality or access issues to consider?	b) What is already in place in the policy or its implementation to address any inequalities or barriers to access including under representation at clinics, screening?	c) Please state any barriers that still need to be addressed and any proposed actions to eliminate inequality
The area of policy or its implementation being assessed:			
Race and Ethnicity:	None	Not applicable	None
Gender:	None	Not applicable	None
Age:	None	Not applicable	None
Religion:	None	Not applicable	None
Disability:	Visual accessibility of this policy	Already in Arial font size 12. Use of technology by end user. This policy can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request	None
Sexuality:	None	Not applicable	None
Pregnancy and Maternity:	None	Not applicable	None
Gender Reassignment:	None	Not applicable	None
Marriage and Civil Partnership:	None	Not applicable	None
Socio-Economic Factors (i.e. living in a poorer neighbourhood / social deprivation):	None	Not applicable	None

What consultation with protected characteristic groups including patient groups have you carried out? • None
What data or information did you use in support of this EqIA? • Trust guidance for completion of the Equality Impact Assessments
As far as you are aware are there any Human Rights issues be considered such as arising from surveys, questionnaires, comments, concerns, complaints or compliments? • No

<u>Level of impact</u> From the information provided above and following EqIA guidance document please indicate the perceived level of impact: Low Level of Impact

Name of Responsible Person undertaking this assessment: Information Governance Manager
Signature: G.H.Robinson
Date: 24th July 2023

8 APPENDICES

Appendix A – Definitions

Anonymised data	Anonymisation is the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified
Confidential information	Confidential information can be anything that relates to patients, staff or any other information (such as medical and staff records, contracts, tenders, etc.) held either in paper, disc, computer file or printout, video, photograph or even heard word of mouth. It includes information stored on portable devices such as laptops, mobile telephones and external hard drives/memory sticks). Personal information that is subject to a duty of confidence has a number of characteristics, i.e., the information: • is not in the public domain or readily available from another source. • has a certain degree of sensitivity, (more than gossip) such as medical history. • has been provided with the expectation that it will only be used or disclosed for particular purposes. This expectation may arise because a specific undertaking has been given, because the confider places specific restrictions on the use of data which are agreed by the recipient, or because the relationship between the recipient and the data subject generally gives rise to an expectation of confidentiality, for instance as arises between a patient and doctor. This is a term used in the Caldicott Information Governance Review and describes personal information about identified or identifiable individuals, which should be kept private or secret and includes deceased as well as living people. The review interpreted 'personal' as including the Data Protection Act definition of personal data but included data relating to the deceased as well as living people, and '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.
Explicit consent	If confidential patient information is used for purposes beyond individual care, for example a research project, then it will normally be necessary for staff to obtain explicit consent. This is a very clear and specific statement of consent. It can be given in writing, verbally

	or through another form of communication such as sign language.
Implied consent	If confidential patient information is accessed and used for individual care then consent is implied, without the patient having to explicitly say so. This is because it is reasonable for patients to expect that relevant confidential patient information will be shared with those caring for them on a need-to-know basis.
Personal Data	Personal data means information about a particular living individual 'data subject'. It does not need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data. It does not cover truly anonymous information – but if you could still identify someone from the details, or by combining it with other information, it will still count as personal data. It only includes paper records if we plan to put them on a computer (or other digital device) or file them in an organised way. In the Trust, all paper records are technically included – but will be exempt from most of the usual data protection rules for unfiled papers and notes. Examples of personal information include: • a name • an identification number i.e., NHS number, NI number • location data • an online identifier ie. IP addresses and cookie identifiers • one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Name, address, postcode, email address, date of birth, NHS number, National Insurance number, passport/driving licence numbers.
Processing	Almost anything we do with data counts as processing, including collecting, recording, storing, using, analysing, combining, disclosing or deleting it. Receipt and despatch of confidential information.
Pseudonymised data	Pseudonymisation is defined within the GDPR as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject

	without the use of additional information i.e., NHS number, name, date of birth, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable individual".
Safe Haven	The term 'Safe Haven' is used within the NHS to denote either a secure physical location or the agreed set of administrative arrangements that are in place to ensure security classified, personal or other sensitive information is communicated safely and securely.
Special categories of personal data (or information, previously known as sensitive data, Data Protection Act 1998, 2018)	The special categories of personal data are: a) racial or ethnic origin b) political opinions c) religious or philosophical beliefs d) trade-union membership e) genetic data f) biometric data for the purpose of uniquely identifying a natural person. g) data concerning health. h) data concerning a natural person's sex life or sexual orientation. • Biometrics • Criminal convictions • Ethnic origin • Genetics • Health information • Politics • Race • Religious beliefs • Sexual life • Sexual orientation • Trade union membership For this type of information even more stringent measures should be employed to ensure that the date remains secure.

Appendix B – Application to Access Health Records

Healthier Communities, Outstanding Care

Application to Access Health Records (DPA1)

NHS Sherwood Forest Hospitals NHS Foundation Trust

Before completion, please read our accompanying leaflet 'Accessing Health Records' for important information on your rights to access and timescales.

PLEASE COMPLETE IN **BLOCK CAPITALS AND DARK INK**

1. The Patient

FULL NAME (Including Title)			
PREVIOUS NAME		**DATE OF BIRTH**	DD/MM/YY
HOSPITAL / NHS NUMBER	IF KNOWN		
CURRENT ADDRESS – INC POSTCODE		**PREVIOUS ADDRESS – INC POSTCODE**	
TELEPHONE NUMBER		**MOBILE NUMBER**	

2. For completion by the APPLICANT

□ Please tick if you are the patient and go straight to Section 3A. **If you are not the patient, please complete section 2.1.**

2.1 FULL NAME (Including Title)			
PREVIOUS NAME		**DATE OF BIRTH**	DD/MM/YY
RELATIONSHIP TO PATIENT			
CURRENT ADDRESS – INC POSTCODE		**PREVIOUS ADDRESS – INC POSTCODE**	

TELEPHONE NUMBER		**MOBILE NUMBER**	

3. Declaration (please tick as appropriate)

You are advised that the making of a false or misleading statement in order to obtain access to personal information to which you are not entitled is a criminal offence.
I declare that the information given by me is correct to the best of my knowledge, that I am entitled to apply for access to health records referred to under the terms of the General Data Protection Regulation 2018 and that:

A	**I am the patient** (After signing in section 3.1 please go to section 4)	
B	**I have been asked to apply by the patient and completed within this form is the patient's written consent** (After signing in section 3.1 and 3.2 please go straight to section 4)	
C	**I am the patient's legally appointed personal representative and I attach confirmation of my appointment (e.g., Power of Attorney for Health)** (See 3.1 of the information for patients leaflet, *Accessing Health Records*) (After signing in section 3.1 please go straight to section 4)	
D	**I have parental responsibility for a child under the age of 18, who is not competent to understanding the request and give their consent.** (See Section 8 of the information for patients leaflet, *Accessing Health records*) (After signing in section 3.1 please go straight to section 4)	
E	**I have parental responsibility for a child under the age of 18, who has consented to my making this request and has completed the written authorisation below.** (Please note children aged 16 and 17 are regarded as adults for this purpose, and their consent must be obtained before a person with parental responsibility can be given access to their health records). (See section 8 of the Information for Patients leaflet, *Accessing Health Records*) (After signing in section 3.1 and 3.2 please go straight to section 4)	
F	**The patient is deceased, and I am the deceased patient's personal representative and I attach confirmation/documentary evidence of my appointment (e.g. Grant of Representation from the Probate Service or Letters of Administration)** (See 3.2 of the Information for Patients leaflet, *Accessing Health Records*) (After signing in section 3.1 please go straight to section 4)	
G	**I have evidence arising from the patient's death and I attach documentary evidence.** (See 3.2 of the Information for Patients leaflet, *Accessing Health Records*) (After signing in section 3.1 please go straight to section 4)	
H	**Relevant to my claim on the grounds that: -** (Please detail) _____ _____ (After signing in section 3.1 please go to section 4)	

3.1Signature of Applicant: …… Date: ……

(As indicated in Section 2)

3.2 Patient's written consent

To be completed if the Patient is giving the Applicant their consent to apply:
I hereby authorise Sherwood Forest Hospital NHS Foundation Trust to release my personal information as specified within this application to:

Name: …….. to whom I give consent to act on my behalf.

Signature of Patient: …… Date: …….
(as indicated in Section 1)

Please note: There are now **no fees** to be paid in order to access your medical notes under the UK General Data Protection Regulation.

We do require identification when requesting any medical records. This is to ensure that all patient data is kept secure and is in accordance with our trust policy. Please see Section 4 for details.

4. Proof of Identity of the Patient/Applicant

It is essential to provide adequate proof of identification to permit us to establish your right of access to information under the General Data Protection Regulation 2018.
Please remember to submit the following documents when you submit this application.
EXAMPLES OF ACCEPTABLE DOCUMENTS:

- **If you are requesting copies of your own health records** (as indicated in Section 1)
  - □ 1 item to confirm your signature ***AND***
  - □ 1 item to confirm your address

Signature Documents	***Address Documents***
Passport	**Utility Bill**
Driving Licence	**Council Tax Bill**
	Bank Statement
	Credit Card Statement
	Insurance Letters/Docs

- **If you are requesting copies of health records on behalf of a patient** (as indicated in Section 2)
  - □ 1 Item to confirm the patient's signature
  - □ 1 Item to confirm the patient's address
  - □ 1 item to confirm your signature
  - □ 1 item to confirm your address

- **If you are requesting copies of a child's health records**
  - □ Birth Certificate or Passport for Child
  - □ 1 Item to confirm your signature
  - □ 1 Item to confirm your address

- **If you are requesting copies of health records of a deceased person**
  - □ 1 Item to confirm your signature
  - □ 1 Item to confirm your address
  - □ A copy of the Representation document confirming your appointment (e.g., Grant of Probate) ***OR*** evidence of your claim arising from the patient's death (e.g. Letter of instruction to Solicitor)

- **If you are requesting copies of health records for a patient that is not able to manage their own affairs**
  - □ 1 Item to confirm your signature
  - □ 1 Item to confirm your address
  - □ Copy of the Lasting Power of Attorney Document (LPA)

Signature Documents	***Address Documents***	***Representation Documents***
Passport	**Utility Bill**	Grant of Probate
Driving Licence	**Council Tax Bill**	Letters of Administration
Child's Documents	Bank Statement	Copy Of Will
Birth Certificate	Credit Card Statement	Power of Attorney
Passport	Insurance Letters/Docs	

5. What information do you require?

We ask that you provide as much information as possible, giving full details of the information you wish to have access to. Please inform us specifically of which information you would like, it will help us deal with your enquiry more promptly and will keep the cost of supplying copies to a minimum.

Department / Ward / Clinic	Consultant	Date(s) of Episode
Any other details:		

I require (please tick):

□ Copies of written information only (health records)
□ Copies of computer data only
□ Copies of both computer data and written information
□ Copies of radiology images (x-rays & scans)
□ I want to **view only written records** and supply of copies is not required (See Section 10 of the Information for Patients Leaflet, *Accessing Health Records*)
□ I want to **view only computer record**s and supply of copies is not required (See Section 10 of the Information for Patients leaflet, *Accessing Health Records*)
□ If you require copies of your records for a Department of Social Security Tribunal, please indicate here:

_____
_____
_____
_____
_____

Should you require any further assistance on how to complete this application form, please do not hesitate to contact us by phone or email.

PLEASE NOTE:

Your application will be processed upon receipt of the completed application form and relevant ID. Failure to forward the required proof of identity may result in a *delay/refusal of your application*.

When you have completed the application and have the relevant ID, please bring/post/email your form to:

Access to Health Records
Sherwood Forest Hospitals NHS Foundation Trust
Kings Mill Hospital
Mansfield Road
Sutton In Ashfield
Nottinghamshire
NG17 4JL

Tel: 01623 672231 or 01623 622515 ext. 3233 or 3235
Email: sfh-tr.sar@nhs.net

Appendix C – Using Personal Data for non-healthcare purposes checklist.

1. What is the purpose of the processing? Describe the project in more detail, who are you sharing data with?	
2. Has IAO// Caldicott Guardian/ Senior Information Risk Owner/Data Protection Officer advice and approval been obtained?	
3. Is using identifiable data justified? Ie name, address, date of birth, NHS Number	
4. If yes, what is the minimum data required? Ie use the NHS number and remove other personal data?	
5. If not, will the data be anonymised[20] or pseudonymised[21]?	
6. If pseudonymised, will the Trust hold the key?	
7. Where will the data be stored? Ie The Trust or offsite with a supplier?	
8. Is the asset (system, process) registered in the Division/ Department's Information Asset Register?	
9. Who will have access to the data?	
10. Will identifiable data be transferred?	
11. If so, how will this be kept secure in transit i.e., HL7[22]?	
12. Are outputs from the processing anonymised?	
13. If not, why?	
14. What will happen to the data when it is no longer required?[23][24]	
15. Are all staff who have access to this personal data up to date with their Information Governance training?	

[20] Anonymisation is the process of removing personal identifiers, both direct and indirect, that may lead to an individual being identified.
[21] Pseudonymisation is defined within the GDPR as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information i.e., NHS number, name, date of birth, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution to an identified or identifiable individual".
[22] https://digital.nhs.uk/services/fhir-apis
[23] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=9855
[24] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8647