

DATA PROTECTION IMPACT ASSESSMENT POLICY

POLICY

Reference	IG/007		
Approving Body	Data Protection and Cyber Security Committee		
Date Approved	17 th November 2025		
For publication to external SFH website	Positive confirmation received from the approving body that the content does not risk the safety of patients or the public:		
	YES	NO	N/A
	X		
Issue Date	January 2026		
Version	3		
Summary of Changes from Previous Version	Updates to definitions/abbreviations specifically to include Artificial Intelligence, Machine Learning, Data Leakage and Data (Use and Access) Act 2025 Updates to the Process of Using CoreStream to complete DPIAs		
Supersedes	2		
Document Category	Information Governance		
Consultation Undertaken	Information Governance Working Group		
Date of Completion of Equality Impact Assessment	October 2025		
Date of Environmental Impact Assessment (if applicable)	Not applicable		
Legal and/or Accreditation Implications	Failure to undertake could result in enforcement action		
Target Audience	All staff and members of the public		
Review Date	2 years or earlier if updates are required.		
Sponsor (Position)	Director of Corporate Affairs		
Author (Position & Name)	Jacquie Widdowson, Head of Data Security and Privacy		
Lead Division/ Directorate	Corporate		
Lead Specialty/ Service/ Department	Information Governance		
Position of Person able to provide Further Guidance/Information	Information Governance Team and Head of Data Security and Privacy		
Associated Documents/ Information		Date Associated Documents/ Information was reviewed	
1. Data Protection Impact Assessment Procedure		November 2025	
Template control		April 2024	

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 sfh-tr.information.governance@nhs.net

Contents

1.0	INTRODUCTION	3
2.0	POLICY STATEMENT.....	4
3.0	DEFINITIONS/ ABBREVIATIONS	5
4.0	ROLES AND RESPONSIBILITIES	8
5.0	APPROVAL.....	9
6.0	DOCUMENT REQUIREMENTS	9
6.1	WHEN IS A DATA PROTECTION IMPACT ASSESSMENT MANDATORY?	9
6.2	WHEN IS A DATA PROTECTION IMPACT ASSESSMENT NOT REQUIRED?	12
6.3	AT WHAT STAGE DO I COMPLETE A DATA PROTECTION IMPACT ASSESSMENT?	12
6.4	WHO IS REQUIRED TO CARRY OUT THE DATA PROTECTION IMPACT ASSESSMENT?	12
6.5	HOW TO CONDUCT A DATA PROTECTION IMPACT ASSESSMENT	13
6.5.1	THE PROCESS OF THE DPIA WITHIN CORESTREAM.....	13
6.6	WHEN DO WE NEED TO CONSULT THE INFORMATION COMMISSIONER'S OFFICE?	14
7.0	MONITORING COMPLIANCE AND EFFECTIVENESS	15
8.0	TRAINING AND IMPLEMENTATION.....	16
8.1	Training.....	16
8.2	Implementation.....	16
9.0	IMPACT ASSESSMENTS	16
10.0	EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS	16
11.0	KEYWORDS.....	18
12.0	APPENDICES	18
	APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)	19
	APPENDIX 2 SCREENING QUESTIONS	21
	APPENDIX 3 DPIA QUESTIONS	23

1.0 INTRODUCTION

A Data Protection Impact Assessment (DPIA) is a process designed to help organisations analyse, identify and minimise the Data Protection risks¹ of a project or plan. It is a key part of our accountability obligations under UK General Data Protection Regulation (UK GDPR), and when done properly helps the Trust assess and demonstrate how the organisation complies with Data Protection obligations.

It does not have to eradicate all risk but should help minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve. An effective Data Protection Impact Assessment (DPIA) allows you to identify and fix problems at an early stage, bringing broader benefits for both individuals and the Trust.

It can reassure individuals that we are protecting their interests and have reduced any negative impact on them as much as we can. In some cases, the consultation process for a Data Protection Impact Assessment (DPIA) will give individuals a chance to have some say in the way their information is used. Conducting and publishing a Data Protection Impact Assessment (DPIA) can also improve transparency and make it easier for individuals to understand how and why we are using their information.

Conducting a Data Protection Impact Assessment (DPIA) will help us to build trust and engagement with the people using our services, and improve our understanding of their needs, concerns and expectations.

A Data Protection Impact Assessment (DPIA) can cover a single processing operation, or a group of similar processing operations. You may even be able to rely on an existing Data Protection Impact Assessment (DPIA) if it covered a similar processing operation with similar risks. A group of organisations can also do a joint Data Protection Impact Assessment (DPIA) for a group project or industry-wide initiative.

For new technologies, you may be able to use a Data Protection Impact Assessment (DPIA) done by the product developer to inform your own Data Protection Impact Assessment (DPIA) on your implementation plans.

For new projects, Data Protection Impact Assessments (DPIA) is a vital part of Data Protection by design. They build in Data Protection compliance at an early stage, when there is most scope for influencing how the proposal is developed and implemented.

However, it's important to remember that Data Protection Impact Assessments (DPIA) are also relevant if you are planning to make changes to an existing system. In this case you must

¹ Risk in this context is about the potential for any significant physical, material or non-material harm to individuals

ensure that you do the Data Protection Impact Assessment (DPIA) at a point when there is a realistic opportunity to influence those plans.

In other words, a Data Protection Impact Assessment (DPIA) is not simply a rubber stamp or a technicality as part of a sign-off process. It's vital to integrate the outcomes of your Data Protection Impact Assessment (DPIA) back into your project plan.

You should not view a Data Protection Impact Assessment (DPIA) as a one-off exercise to file away. A Data Protection Impact Assessment (DPIA) is a 'living' process to help you manage and review the risks of the processing and the measures you've put in place on an on-going basis. You need to keep it under review and reassess if anything changes.

In particular, if you make any significant changes to how or why you process personal data, or to the amount of data you collect, you need to show that your Data Protection Impact Assessment (DPIA) assesses any new risks. An external change to the wider context of the processing should also prompt you to review your Data Protection Impact Assessment (DPIA). For example, if a new security flaw is identified, new technology is made available, or a new public concern is raised over the type of processing you do or the vulnerability of a particular group of individuals.

Under UK General Data Protection Regulation (UK GDPR), failure to carry out a Data Protection Impact Assessment (DPIA) when required may leave the Trust open to enforcement action, including a fine of up to £17.5 million, or 4% of annual global turnover, whichever is greater.

There can also be financial benefits. Identifying a problem early on generally means a simpler and less costly solution, as well as avoiding potential reputational damage later on. A Data Protection Impact Assessment (DPIA) can also reduce the on-going costs of a project by minimising the amount of information you collect where possible and devising more straightforward processes for staff.

2.0 POLICY STATEMENT

Sherwood Forest Hospitals NHS Foundation Trust (the Trust) processes a significant volume of personal and special category of data including data relating to children and vulnerable adults. In compliance with Article 25 of the GDPR the Trust adopts internal policies and implements measures which meet the principles of data protection from the initiation of new projects into the Trust.

Adhering to this policy, using the relevant documentation associated we will be able to identify when a Data Protection Impact Assessment (DPIA) is required and/or appropriate and record the process through to completion of a Data Protection Impact Assessment (DPIA) for ratification.

For this policy to be its most effective, it must be followed at the very early planning stages of new projects and run alongside the project plan.

3.0 DEFINITIONS/ ABBREVIATIONS

Anonymised Data	Anonymised data refers to personal information that has been modified in such a way that individuals can no longer be identified
Artificial Intelligence (AI)	Artificial intelligence (AI) refers to the ability of computer systems to perform tasks that typically require human intelligence, such as learning, reasoning, decision-making, and problem-solving.
Data Controller	Sherwood Forest Hospitals NHS Foundation Trust is registered as a Data Controller with the Information Commissioner's Office. A Data Controller is defined as 'a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are or are to be processed'.
Data flow	Data flow within a system describes the path and transformation of data as it moves between components, such as from a source to a process, and then to a storage or destination, with data flow diagrams (DFDs) used to visually map these journeys.
Data Leakage	Data Leakage refers to the potential risk for data being leaked to services and/or unintended audiences.
Data Processor	A processor is a natural or legal person (not an employee), public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority. In doing so, they serve the controller's interests rather than their own.
Data Protection Act 2018	The Data Protection Act 2018 controls how your personal information is used by organisations, businesses or the government. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR).
Data subject	This is the technical term for the individual whom particular personal data is about. In this policy we generally use the term 'patients and staff' instead.
DUAA	Data (Use and Access) Act 2025
Human Rights Act 1998	The Human Rights Act 1998 requires that any intrusion into the private and family life of an individual must be in accordance with the law, proportionate and necessary for: <ul style="list-style-type: none"> • national security • public safety • the economic well-being of the country

	<ul style="list-style-type: none"> for the prevention of disorder or crime for the protection of health or morals or for the protection of the rights and freedoms of others.
ICO (Information Commissioner's Office)	The ICO is the supervisory authority for Data Protection in the UK. They offer advice and guidance, promote good practice, monitor breach reports, conduct audits and advisory visits, consider complaints, monitor compliance and take enforcement action where appropriate.
Information Asset	A body of information that is defined and managed as a single unit, so that it can be understood, protected, used and shared effectively.
Information Asset Administrator (IAA)	Information Asset Administrator. IAAs are operational staff with day-to-day responsibility for managing risks to their information asset(s).
Information Asset Owner (IAO)	Information Asset Owner. IAOs are senior individuals responsible for maintaining good Data Protection and Security/Information Governance arrangements and standards within the relevant business/service areas of the Trust for which they have responsibility.
Information Asset Register (IAR)	Information Asset Register. The Trust's information asset register is stored within Corestream and populates when completing the DPIA.
Machine Learning (ML)	Machine Learning is a type of technology within Artificial Intelligence (AI) that allows computer systems to learn from data. Instead of being programmed with specific instructions, these systems can recognise patterns and make decisions or predictions based on new information.
Personal data²	<p>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.</p> <p>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.</p> <p>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.</p> <p>Examples of personal information include:</p> <ul style="list-style-type: none"> a name identification number i.e. NHS number, NI number location data an online identifier i.e. 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.

² Personal information and personal data are used interchangeably in this document

Processing	Almost anything we do with data counts as processing, including collecting, recording, storing, using, analysing, combining, disclosing or deleting it.
Pseudonymised Data	Pseudonymised data refers to personal information from which direct identifiers have been removed or replaced with artificial substitutes, such as a reference number. This means the data cannot be linked to a specific individual without access to additional, separate information.
Special categories of personal data	The special categories of personal data are: <ul style="list-style-type: none"> 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.
Third Party	Any person, agency/organisation authorised by the data controller to process data for a specified purpose on their behalf.
UK GDPR	In the UK, data protection is governed by the UK General Data Protection (UK GDPR)

4.0 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 policy.

Data Protection and Cyber Security 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 policy 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 Data Protection and Cyber Security Committee.

Senior Information Risk Owner (SIRO)

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 Chief Medical Officer 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 (DPO)

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 takes into account the nature, scope, context and purposes of processing.

Chief Clinical Information Officer

Liaises between clinical medicine, IT and information management and provides guidance and leadership to ensure the Data Protection Impact Assessment is implemented.

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.

All Staff

All Trust employees and anyone else working for The Trust (e.g. agency staff, honorary staff, management consultants etc.) who use and have access to Trust personal information must understand their responsibilities for Data Protection and confidentiality.

5.0 APPROVAL

Policy approval is by the Data Protection and Cyber Security Committee.

6.0 DOCUMENT REQUIREMENTS

6.1 WHEN IS A DATA PROTECTION IMPACT ASSESSMENT MANDATORY?

Conducting a Data Protection Impact Assessment (DPIA) is a legal requirement for any type of processing, including certain specified types of processing that are likely to result in a **high risk³ to the rights and freedoms of individuals**.

³ To assess whether something is 'high risk', the GDPR is clear that you need to consider both the likelihood and severity of any potential harm to individuals. 'Risk' implies a more than remote chance of some harm. 'High risk' implies a higher threshold, either because the harm is more likely, or because the potential harm is more severe, or a combination of the two.

In order to provide a more concrete set of processing operations that require a Data Protection Impact Assessment (DPIA), the following twelve criteria points should be considered. **In most cases, a combination of two of the twelve factors indicates the need for a Data Protection Impact Assessment (DPIA). However, in some cases, the Trust can consider meeting only one of the twelve factors.** The Data Protection Impact Assessment Procedure is available on the Trust's website⁴ You will need to complete a set of screening questions within CoreStream⁵ which will determine if you need to complete the Full Data Protection Impact Assessment:

1. **Evaluation or scoring** - including profiling and predicting. For example, a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks.
2. **Automated decision making with legal or similar significant effect** - processing that aims at taking decisions on individuals. For example, the processing may lead to the exclusion or discrimination against individuals.
3. **Systematic monitoring** of individuals - processing used to observe, monitor or control individuals. For example, CCTV, monitoring of the employees' workstation, internet activity, etc.
4. **Sensitive data or data of a highly personal nature** - this includes special categories of personal data (for example information about individuals' health care, racial or ethnic origin etc.).
5. **Data processed on a large scale** –
 - a. how many individuals concerned, either as a specific number or as a proportion of the relevant population.
 - b. the volume of data and/or the range of different data items being processed.
 - c. the duration, or permanence, of the data processing activity.
 - d. the geographical extent of the processing activity.
6. **Matching or combining datasets** - for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the reasonable expectations of the data subject⁶

⁴ <https://www.sfh-tr.nhs.uk/media/ae2j4tns/data-protection-impact-assessment-procedure.pdf>

⁵ https://sfh-idserver.corestream.co.uk/Acc/Login?ReturnUrl=%2Fconnect%2Fauthorize%2Fcallback%3Fclient_id%3Dvue%26redirect_uri%3Dhttps%253A%252F%252Fsfh.corestream.co.uk%252Flogincallback%26response_type%3Dcode%26scope%3Dopenid%2520profile%2520email%2520api%26state%3D1cdf30b68bfc41bba1993c62fd7b0120%26code_challenge%3DFzXMtK7OBIMJvS4sN07RnKOeVD6f_2DKYfeqjS0tfS0%26code_challenge_method%3DS256%26response_mode%3Dquery

⁶ See explanation in the WP29 Opinion on Purpose limitation 13/EN WP 203, p.24
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

7. **Data concerning vulnerable individuals** - individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable individuals may include children, employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.).
8. **Innovative use or applying new technological or organisational solutions** - combining the use of fingerprint and face recognition for improved physical access control.
9. **Preventing individuals from exercising a right or using a service or contract** - When the processing in itself “prevents individuals from using a service or a contract”. An example of this is where a bank screens its customers against a credit reference database in order to decide whether to offer them a loan.
10. **Offer online services directly to children** - Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved. If you process children’s personal data, then you should think about the need to protect them from the outset and design your systems and processes with this in mind.
11. **Storing or transmitting data outside the EU/EEA** - You may make a restricted transfer if the receiver is located in a third country or territory, or is an international organisation, or in a particular sector in a country or territory, covered by UK 'adequacy regulations'. You can make a restricted transfer if it is covered by a legal instrument between public authorities or bodies containing ‘appropriate safeguards’. The appropriate safeguards must include enforceable rights and effective remedies for people whose personal data is transferred.
12. **Direct marketing e.g. newsletters, email subscriptions** - Direct marketing can add value to the customer experience. It can make people aware of new products and services that they may benefit from, give them opportunities to take part in events, or find out about important causes. When done responsibly direct marketing can also increase trust and confidence in your brand or organisation. However, direct marketing has the potential to cause nuisance to people, and in some cases, it can cause them harm and distress.

Data Protection Impact Assessments should be conducted on any plan or proposal for a system or service where privacy issues may need to be considered. It does not have to be a formal project as a Data Protection Impact Assessment is suitable for:

- A new IT system for storing and accessing personal data.
- A data sharing initiative between organisations to pool or link sets of personal data.
- A proposal to identify people in a particular group or demographic and initiate a course of action.
- Using existing data for a new and unexpected or more intrusive purpose.
- A new surveillance system or the application of new technology to an existing system.
- A new database that consolidates information held by separate parts of an organisation.

- Legislation, policy or strategies, which will affect privacy through the collection of use of information, or through surveillance or other monitoring.
- Change of use of a building i.e. new reception area, new ward etc.
- Any change in procedure of handling, obtaining, recording using storing, and destruction of personal identifiable data.

6.2 WHEN IS A DATA PROTECTION IMPACT ASSESSMENT NOT REQUIRED?

A Data Protection Impact Assessment is not required in the following cases:

- where the project is unlikely to result in a high risk to the rights and privacy of individuals.
- when the nature, scope, context and purposes are very similar to a project for which a Data Protection Impact Assessment (DPIA) has been carried out. In such cases, results of previous Data Protection Impact Assessments (DPIA) can be used.
- where the processing is included on the optional list. This list at the time of writing this policy is not available from the Information Commissioner's Office.

6.3 AT WHAT STAGE DO I COMPLETE A DATA PROTECTION IMPACT ASSESSMENT?

The Data Protection Impact Assessment should be carried out “**prior to the processing**”.

The Data Protection Impact Assessment (DPIA) should be started as early as possible in the project, even if some of the finer details are still unknown. Updating the Data Protection Impact Assessment (DPIA) throughout the project will ensure that data protection and privacy are considered and will encourage the creation of solutions which promote compliance. It can also be necessary to repeat individual steps of the assessment as the development process progresses.

The Data Protection Impact Assessment (DPIA) is an on-going process, especially where a project is dynamic and subject to on-going change. Carrying out a Data Protection Impact Assessment (DPIA) is a continual process, not a one-time exercise.

6.4 WHO IS REQUIRED TO CARRY OUT THE DATA PROTECTION IMPACT ASSESSMENT?

The Trust is responsible for ensuring that the Data Protection Impact Assessment (DPIA) is carried out. The Data Protection Impact Assessments (DPIA) may be done by someone else, inside or outside the organisation, but the Trust remains ultimately accountable. Data Protection Impact Assessments should be completed by Information Asset Owners/Administrators who have good knowledge of the project, the systems involved, and the level of information required. It is likely that multiple staff from the project will need to be involved with carrying out the Data Protection Impact Assessment.

The Trust must also seek the advice of the Data Protection Officer (DPO), and this advice, and the decisions taken by the Trust, should be documented within the Data Protection Impact Assessment (DPIA). The Data Protection Officer should also monitor the performance of the Data Protection Impact Assessment (DPIA).

If the project is wholly or partly performed by a third party (data processor), **the third party should assist the Trust in carrying out the Data Protection Impact Assessment (DPIA)** and provide any necessary information.

The Trust must also “**seek the views of data subjects (individuals) or their representatives**”, where appropriate”. The Trust should also document its reasoning for not seeking the views of individuals, if it decides that this is not appropriate, for example if doing so would compromise the confidentiality of companies’ business plans or would be disproportionate or impracticable.

In risk management terms, a Data Protection Impact Assessment (DPIA) aims at “managing risks” to the rights and freedoms of individuals, using the following processes, by:

- establishing the context: “taking into account the nature, scope, context and purposes of the processing and the sources of the risk”.
- assessing the risks: “assess the particular likelihood and severity of the high risk”.
- treating the risks: “mitigating that risk” and “ensuring the protection of personal data”, and “demonstrating compliance”.
-

6.5 HOW TO CONDUCT A DATA PROTECTION IMPACT ASSESSMENT

Data Protection Impact Assessments are completed within CoreStream⁷ which is accessed online. You will need to contact the Information Governance Team⁸ to provide you access to the system if you do not have this already.

6.5.1 THE PROCESS OF THE DPIA WITHIN CORESTREAM

1. Complete the screening questions within CoreStream to determine whether a full DPIA is necessary.
1. If a full DPIA is required, CoreStream will automatically generate the additional questions within the DPIA form.
2. Submit the completed DPIA to Information Governance (IG) Team for initial review.

⁷ [Welcome to CoreStream](#)

⁸ Information Governance Team sfh-tr.information.governance@nhs.net

3. After review by a member of the IG Team, the DPIA will be forwarded to the Information Governance Working Group (IGWG) for broader consultation.
4. Once any feedback from the IGWG has been incorporated, the DPIA will proceed to the Data Protection and Cyber Security Committee for final approval.
5. Following Data Protection and Cyber Security Committee approval, your product/system can be implemented within the Trust. NOTE – No product/system should be implemented without the correct authorisation.
6. Review and update your DPIA annually, or sooner if any changes occur whichever comes first.

6.6 WHEN DO WE NEED TO CONSULT THE INFORMATION COMMISSIONER'S OFFICE?

If you identify a high risk that you cannot take measures to reduce, the Data Protection Officer must consult the Information Commissioner's Office. You cannot begin the processing. The Information Commissioner's Office will give written advice within eight weeks, or fourteen weeks in complex cases. If appropriate, they may issue a formal warning not to process the data or ban the processing altogether.

An example of an unacceptable high residual risk includes instances where the individuals may encounter significant, or even irreversible, consequences, which they may not overcome (e.g.: an illegitimate access to data leading to a threat on the life of the individuals, a layoff, a financial jeopardy) and/or when it seems obvious that the risk will occur (e.g.: by not being able to reduce the number of people accessing the data because of its sharing, use or distribution modes, or when a well-known vulnerability is not patched).

7.0 MONITORING COMPLIANCE AND EFFECTIVENESS

Minimum Requirement to be Monitored	Responsible Individual	Process for Monitoring e.g. Audit	Frequency of Monitoring	Responsible Individual or Committee/ Group for Review of Results
(WHAT – element of compliance or effectiveness within the document will be monitored)	(WHO – is going to monitor this element)	(HOW – will this element be monitored (method used))	(WHEN – will this element be monitored (frequency/ how often))	(WHERE – Which individual/ committee or group will this be reported to, in what format (e.g. verbal, formal report etc) and by who)
Audit of completed Data Protection Impact Assessments (DPIAs)	Information Governance Team	Audit	Annually	Data Protection and Cyber Security Committee
Adherence to Information Governance policies and procedures in nominated Division/ Department	360 Assurance	Audit	Annually	Data Protection and Cyber Security Committee

8.0 TRAINING AND IMPLEMENTATION

8.1 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 or online⁹. 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](#).

All staff who are granted access to CoreStream will be provided training on using the system and the relevant modules by the Information Governance team.

8.2 Implementation

A copy of this policy and all related policies and procedures are provided to all staff and patients on the Trust's website¹⁰.

9.0 IMPACT ASSESSMENTS

- This document has been subject to an Equality Impact Assessment, see completed form at Appendix 1
- This document is not subject to an Environmental Impact Assessment

10.0 EVIDENCE BASE (Relevant Legislation/ National Guidance) AND RELATED SFHFT DOCUMENTS

Evidence Base:

- Confidentiality: NHS Code of Practice
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf
- Data Protection Act 2018 <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>

⁹ [Log in to the site | Sherwood eAcademy](#)

¹⁰ <https://www.sfh-tr.nhs.uk/about-us/regulatory-information/non-clinical-policies/> <https://www.sfh-tr.nhs.uk/about-us/regulatory-information/clinical-policies/>

- Data Use and Access Act 2025 <https://bills.parliament.uk/bills/3825>
- Freedom of Information Act 2000 <https://www.legislation.gov.uk/ukpga/2000/36/contents>
- Health and Social Care Act 2012
<http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted>
- Human Rights Act 1998 <https://www.legislation.gov.uk/ukpga/1998/42/contents>
- Information: To share or not to share? The Information Governance Review March 2013
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf
- International standards e.g. ISO 31000:2009, Risk management — Principles and guidelines, International Organization for Standardization (ISO); ISO/IEC 29134 (project), Information technology – Security techniques – Privacy impact assessment – Guidelines, International Organization for Standardization (ISO) <https://www.iso.org/standards.html>
- ISO/IEC 27002:2022 (Information Security Standards)
<https://www.iso.org/standard/75652.html>
- NHS Act 2006 <https://www.legislation.gov.uk/ukpga/2006/41/contents>
- NHS Care Record Guarantee
<https://www.happyhealthylives.uk/download/clientfiles/files/Care-Record-Guarantee.pdf>
- NHS Constitution for England <https://www.gov.uk/government/publications/the-nhs-constitution-for-england>
- The Network and Information Systems Regulations 2018 (UK) [The Network and Information Systems Regulations 2018 \(legislation.gov.uk\)](https://www.legislation.gov.uk/ukpga/2018/12/contents)
- UK General Data Protection Regulation <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/>

Related SFHFT Documents:

- [Account Management and Access Policy](#)
- [Clinical Records Keeping Standards Policy](#)
- [Code of Conduct Leaflet](#)
- [Confidentiality and Audit Policy](#)
- [Corporate Records Policy](#)
- [Data Protection, Confidentiality and Disclosure Policy](#)
- [Data Protection, Confidentiality and Disclosure Procedure](#)
- [Data Protection Impact Assessment Procedure](#)
- [Health Records Management Policy](#)
- [Information Governance Policy](#)
- [Information Security Policy](#)
- [Information Sharing Policy](#)
- [Guidance for Information Asset Owners](#)
- [Retention and Destruction Policy](#)
- [Retention and Destruction Procedure](#)

11.0 KEYWORDS

Cloud storage, off site, information security, confidentiality, integrity, availability, privacy by design.

12.0 APPENDICES

- Please refer to list in contents table.

APPENDIX 1 - EQUALITY IMPACT ASSESSMENT FORM (EQIA)

Name of service/policy/procedure being reviewed: Data Protection Impact Assessment Policy			
New or existing service/policy/procedure: Existing			
Date of Assessment: 16th October 2025			
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? <ul style="list-style-type: none"> • None 			
What data or information did you use in support of this EqlA? <ul style="list-style-type: none"> • Trust guidance for completion of the Equality Impact Assessments. 			
As far as you are aware are there any Human Rights issues be taken into account such as arising from surveys, questionnaires, comments, concerns, complaints or compliments? <ul style="list-style-type: none"> • No 			
Level of impact From the information provided above and following EQIA guidance document Guidance on how to complete an EIA (click here) , please indicate the perceived level of impact: Low Level of Impact			
Name of Responsible Person undertaking this assessment: Gina Robinson			
Signature: Jody Davies			
Date: 16 th October 2025			

DPIA EXPORT

DPIA

DATE



DPIA SCREENING

Title

Owner(s)

Contributor(s)

What is the purpose for this project/process/change request?

Will the project/process/change request involve the collection of new personal identifiable information (PII) about individuals/colleagues?

Will the project /process/change request ask individuals to provide information about themselves?

Will the project/process/change request involve disclosing information about individuals to organisations or people who have not previously had routine access to the information?

Will the project/process/change request use information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Does the project/process/change request involve you using new technology which might be perceived as being privacy intrusive?

Will the project/process/change request result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations?

Will the project/process/change request require you to contact individuals in ways which they may find intrusive?

Will the project/process/change request require you to share personal identifiable information with 3rd parties or contractors?

ATTACHMENTS

Attachments

Comments

DPIA EXPORT

DPIA

DATE



DPIA SCREENING

Title

Owner(s)

Contributor(s)

What is the purpose for this project/process/change request?

Will the project/process/change request involve the collection of new personal identifiable information (PII)

about individuals/colleagues?

Will the project /process/change request ask individuals to provide information about themselves?

Will the project/process/change request involve disclosing information about individuals to organisations or people who have not previously had routine access to the information?

Will the project/process/change request use information about individuals for a purpose it is not currently used for, or in a way it is not currently used?

Does the project/process/change request involve you using new technology which might be perceived as being privacy intrusive?

Will the project/process/change request result in you making decisions or taking action against individuals in ways which can have a significant impact on them?

Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations?

Will the project/process/change request require you to contact individuals in ways which they may find intrusive?

Will the project/process/change request require you to share personal identifiable information with 3rd parties or contractors?

ORGANISATIONAL HIERARCHY (OWNERSHIP)

Organisation Level 1

Organisation Level 2

Organisation Level 3

Organisation Level 4

Organisation Level 5

Executive Owner(s)

Organisation IAO(s)

Organisation IAA(s)

Organisation Viewer(s)

CORE INFORMATION

ID

What is the data processing under consideration in your project/process/change request?

What are the responsibilities linked to the data processing?

Are there standards applicable to the processing?

DATA PROCESSING SCOPE

What information is being processed?

DATA SHARING

Is data being shared?

Who are the Data Subjects?

NECESSITY AND PROPORTIONALITY

Is the data being collected adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed ('data minimisation')?

Select one or more statements that describe how the information will be kept up to date and checked for accuracy and completeness by all organisations involved

Select one or more statements to describe your management of the retention and disposal of data by all organisations.

Are the relevant contractual clauses in place? e.g., Data Protection Act, GDPR.

Will personal and/or sensitive data be transferred to or from a country outside the European Economic Area (EEA)?

PERSONAL RIGHTS OF DATA SUBJECTS

How are the data subjects informed about the processing?

How can data subjects exercise their rights to rectification and erasure?

How can data subjects exercise their rights of access?

How can data subjects exercise their rights to restriction and to object?

CONSULTATION PROCESS

Do you need to consult the ICO before processing? NB: the ICO need to be informed if you cannot mitigate high risks.

Do you need to consult with anyone else in your organisation?

DATA PROTECTION IMPACT ASSESSMENT DECLARATION

Do you confirm that all answers given are a true reflection of the data processes being assessed?

Do you have any additional information to add to this DPIA?

Please set the overall risk level for the DPIA based on your review of the question responses and any associated Risks.

ATTACHMENTS

Attachments

Comments