NHS
Sherwood Forest Hospitals
NHS Foundation Trust

Data Protection Impact Assessment

Contents

Introduction

Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the UK General Data Protection Regulation's fundamental principles and requirements, and forms part of the focus on accountability.

A Data Protection Impact Assessment (DPIA) is a tool that we use to identify and reduce the data protection risks of our processing activities. They can also help us to design more efficient and effective processes for handling personal data.

The UK General Data Protection Regulation requires the Trust to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is 'data protection by design and by default'.

In essence, this means we have to integrate or 'bake in' data protection into our processing activities and business practices, from the design stage right through the lifecycle. This concept is not new and **is now a legal requirement**.

When and who should complete a DPIA?

- A DPIA must be completed wherever there is **a change to an existing process or service** or **if a new process or information asset is introduced** that is likely to involve a new use or significantly changes the way in which personal data, special categories of personal data or business critical information is processed. **No commitments to, or installation of systems, should take place before the DPIA has been signed off.**

- Information Assets Owners (IAO) and Information Assets Administrators (IAA) **must** complete the DPIA.

- Relevant stakeholders (internal and external suppliers) should be consulted throughout the DPIA process.

Who do I send the completed DPIA to for review?

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

What if I need help?

- Please contact the Information Governance Team sfh-tr.information.governance@nhs.net or SFHT Phonebook (nnotts.nhs.uk)

IMPORTANT – PLEASE COMPLETE ALL QUESTIONS. IF YOU THINK A QUESTION DOES NOT APPLY INSERT N/A AND EXPLAIN WHY.

Project title:	CoreStream
Reference number:	
Implementing organisation:	Sherwood Forest Hospitals NHS Foundation Trust
Key contacts involved in the DPIA (name and job title)	Jacquie Widdowson, Head of Data Security and Privacy Jody Davies, Data Protection & Security Compliance Administrator
Information Asset Owner (name and job title)	Jacquie Widdowson, Head of Data Security and Privacy
Information Asset Administrator (name and job title)	Lindsay Lunn, Data Security & Privacy Co-Ordinator

Step 1 – What is the aim of the project being undertaken

Q1	**Project description: Describe in sufficient detail for the project to be understood**	CoreStream is a data management and privacy tool, which aims to ease the administrative burden of the information governance team. It aids the identification, documentation and management of the Trust's information assets and related content and enables the seamless monitoring and execution of actions to deliver the real-time management of information. Keeping all data contained within information asset registers and processing activities (data flow mapping) in one place, removing the need to use spreadsheets.

Q2	**Why are we doing it?** Summarise why there is a need for implementation or change and the benefits it will realise.	Encourages clear ownership for information assets and provides real, independent insight into the safety of our data.

		Transferring Freedom Of Information management from an existing database onto CoreStream. Transferring the management of subject access requests from the unsupported RFI module on Datix onto CoreStream. Replacing the use of spreadsheets and databases within the department and streamlining processes. Improving reporting on data privacy and management. Automatic alerts can be enabled for monitoring of actions and improved reporting. The project will: • **Deliver -** time and efficiency savings through centralised management and information asset reporting. • **Support -** alignment with UK GDPR/DPA 2018 • **Ensure -** compliance with Information Commissioner's Office (ICO) • **Reduce -** ongoing costs from bringing manual processes online. • **Online Information Asset Register** - efficiently manages assets. • **Creates and links information flows -** risks, breaches and actions to information assets. • **Data flow** - mapping processing activities. • **Workflow -** to manage the approval and review of assets. • **Automated asset and information flow risk level** - based on asset and flow characteristics. • **UK GDPR Role Declarations -** Data Protection Impact Assessments, Subject Access Requests and Freedom of Information Requests. • **Third party supplier risk management** - and due diligence. (DTAC) • **Real time** - reporting dashboards

		• **Integration -** with an industry leading data discovery and redaction tool

Q3	**What is the nature of your relationship with the data subject (patient, staff) whose data will be used?** For example, do you provide direct care to the data subjects, are they your patients?	Patient/Members of public data is stored for identification purposes and to link them with their request for SARS/FOIs. Staff data is stored to allow allocation of assigning of tasks/linking to assets.

Q4	**Individuals need to be told how their information is processed.**	
	Have you consulted the data subject or their representative about using this data? If not, please explain why you haven't consulted them?	Details of the use of CoreStream will be added to both the patient and staff privacy notice available on our website.
	Please provide details and an example of how this consent (if appropriate to rely on consent as a legal basis) to processing of their data was given? (Preferably embed document)	Not applicable
	What information will you give individuals informing them of what you are doing with their data? ie this is consent to the processing of their personal data, not consent to treatment	Details of the use of CoreStream will be added to both the patient and staff privacy notices available on our website.
	Is this information covered by our existing fair processing information or leaflet? If Yes, provide details. If No, please provide text to be added to our fair processing information. Patient[1] Staff[2]	Yes We process personal information of Patients/Members of the public who contact the Trust for SARs/FOIs, in order to process the request. This information is only accessed by the Information Governance Team. Data Processed for FOIs: Name Email address

[1] https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/

[2] https://www.sfh-tr.nhs.uk/work-for-us/your-staff-information/

		Data Processed for SARs Full Name DOB Address NHS Number And any other data that is provided as part of the ID process. Retention process Data will be retained by CoreStream for the duration of the contract, then provided to the Trust upon termination of the contract before being securely deleted.
	Explain why you believe they would consider the proposed new use of their data as being reasonable or expected?	The same data is being collected for the same purposes. The change is the system on which it is being stored.

Q5	**Has an assessment been made that the information collected is the minimum required to meet the aim of the project?**	
	Use of data should not be the first resort if the objective can be achieved without its use. You must justify why the use of all the data is necessary and proportionate. For example, do you need to use all the fields, can you not achieve the same objective with fewer data fields and/or a smaller data set?	Yes, below is a spreadsheet detailing all the available modules and the types of data fields present. Patients/members of public data is only collected to carry out the process of the request. Minimal staff data is stored for task/asset allocation. Copy of IAM Product form questions - Feb
	Has consideration been given to how the same objective or outcome may be achieved without using this data or using less data or employing a different method - explain in full?	Yes, CoreStream is an improvement to the current system. Corestream is a data management and privacy tool, which aims to ease the administrative burden of the information governance team. It aids the identification, documentation and management of the Trust's information assets and related content and enables the seamless monitoring and execution of actions to deliver the real-time management of information.

Step 2: What type of data is being processed?

Q6	**Fully describe ALL the data that will be used and justify why they are needed.**	
	Data item ie MRI images, patient, name, address, IP address, NHS/D number	**Why is it necessary?**
	Copy of IAM Product form questions - Feb	Accountability principle under UK GDPR to document processing activities. Provide transparency to our patients and staff.
	Asset register module Staff Name Email	An online asset registers to create new assets (including ROPA's), edit existing ones and view all related content in one view. The ability to link information flows, risks, actions and breaches to assets. Workflow to manage the approval of changes and the asset review cycle. Automated risk profiling of information assets and information flows.
	Information Flow Register module Staff Name Email	An information flow register that enables you to see a complete list of all information flows, linked to assets. The ability to apply various filters to the data, and export to Excel.
	Asset Actions module Staff Name Email	An action's register that enables you to see a complete list of all actions raised against individual assets. The ability to apply various filters to the data such as due date and owner, and export to Excel.
	Asset Risks module Staff Name Email	A risk register that enables you to see a complete list of all risks raised against assets, flows and DPIA's. The ability to apply various filters to the data such as due date and owner, and export to Excel.
	GDPR Role Declarations module Staff Name Email	An area of the system to complete GDPR role declarations for Processors, Controllers and Data Protection Officers.

	Data Protection Impact Assessments module Staff Name Email	An area of the system to complete Data Protection Impact Assessments (DPIA's) and manage associated risks and actions relating to DPIA's.
	Data Integrity Assessment module Staff Name Email	An area of the system to complete DIA's for either a system or process and view the overall risk level and risk alerts for DIA's.
	Third Parties module Company Name Owner Name Email Telephone	An area of the system to generate third party supplier assessments and DTACs. The ability to send third party supplier assessments and DTACs to suppliers for completion.
	Subject Access Requests module Name Email Address DOB NHS/Hospital ID Any other personal data that is provided through ID verification process. Any personal data that is being provided to the Data Subject as a result of the SAR.	An area of the system to view and manage Subject Access Requests (SARs)
	Freedom of Information Act Requests module Name Email Address	An area of the system to view and manage Freedom of Information (FOI) Requests.
	Reports module Staff Name Email	A reporting dashboard to identify and drill down into assets, information flows and risks that require attention. Nine categories of reports: Asset reports, Flow reports, Risk reports, Action reports, Data Role Declaration reports, DPIA reports, Breach reports, SAR reports and FOI reports.
	Guidance module No personal data processed.	Embedded system guidance pages to guide users through the various actions they can perform in the system.
	Administration module Staff Name	An Organisational Hierarchy area of the system to manage your organisational hierarchy and assign

	Email	roles at the organisational hierarchy level (e.g., IAO's, IAA's, Data Compliance Officers and Viewers). A Systems Manager area of the system to capture a list of systems and associated metadata. A Data Classification area of the system to manage your data types (e.g., salary, email address) and data classification types (e.g., personal data, sensitive personal data). Additional pages of reference data to allow the customer to define the set of permissible values to be used by key data fields (including Records of Processing Activities). A User Management tool to create, edit and manage users (including unlocking accounts and deactivating accounts).

Q7	**Will you use special categories of personal data?**	
	political opinions	☒
	racial or ethnic origin	☒
	religious or philosophical beliefs	☒
	trade-union membership	☒
	genetic data	☒
	biometric data for the purpose of uniquely identifying a natural person	☒
	data concerning health	☒
	data concerning a natural person's sex life or sexual orientation	☒

Q8	**Approximately how many individuals will be in the dataset?**	
	<11 individuals	☐
	11 – 50 individuals	☐
	51 – 100 individuals	☐
	101 – 300 individuals	☐
	301 – 500 individuals	☐
	501 - 1,000 individuals	☐
	1,001 - 5,000 individuals	☐
	5,001 - 10,000 individuals	☐
	10,001 - 100,000 individuals	☐
	100,001 or more individuals	☒

Q9	**How large and expansive are the records sets being used, what will it consist of?**
	Electronic files ranging in size due to the nature of the file and content.

Q10	**What geographical area will the data be drawn from or cover?** For example, Mansfield, Ashfield, Newark and Sherwood patients. Derbyshire patients ?
	Predominately Mansfield, Ashfield, Newark, Sherwood and neighboring counties. Potentially out of area.

Q11	**What is the source of this data?**	
	If the data is being taken from an existing system, identify what system that is and what was the originally purpose that data was collected for? How will this data be accessed?	Patient/Member of Public Data subject Data is provided by the requestor sent to the Trust via email to the shared inbox or via post. Staff Data subject. This will be inputted manually by SFH.
	If it is new data/system that is being collected, describe how this data collection will be done i.e. digital, paper, removeable media?	Data will be manually entered into CoreStream by appropriate staff in the Trust.

Q12	**How will this data be used?**	
	Will this data be used or combined with other data sets, if so what are these other data sets?	No.
	What will this data show you that is relevant to the project aim and purpose?	The Data will provide us with identification of the requestor to enable the successful completion of an FOI/SAR. • It will also improve the contact flow between Asset owners and Information Governance Team.
	Describe the access controls in place. Will the supplier also have access to the data?	Multi-factor authentication or Single Sign On, complex passwords, accounts automatically locked out after 3 unsuccessful attempts.

		A limited number of CoreStream staff will have access to the platform to assist with supporting the platform and issue fixing. This will be on a need-to-know basis and accounts will be deactivated when they are no longer required.
	Complete the Account Management and Access Standard Operating Procedure[3] Account Management & Acces	

Q13	**Describe proportionality measures**		
	Explain how the processing achieves your purpose?	CoreStream is a data management and privacy tool, which aims to ease the administrative burden of the information governance team. It aids the identification, documentation and management of the Trust's information assets and related content and enables the seamless monitoring and execution of actions to deliver the real-time management of information.	
	Is there another way to achieve the same outcome, give details of alternatives you have rejected and provide the reasons why?	No, current processes of using paper and spreadsheets are an administrative burden and digitising the processing will enable the Trust to be more efficient.	
	Please explain why a smaller amount of data cannot be used.	The minimum data sets will be used in all CoreStream modules.	
	Does the National Data Opt-Out apply (allows patients to opt out of their confidential patient information being used for research and planning)?	Yes	No
		☐	☒

[3] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=13618

Q14	**What is the duration of this processing?** Is this one-off processing or will it continue for a specified period?
	Processing will remain for the duration of the contract.

Q15	**How long will the data be kept and how will it be deleted?**	
	NHS data needs to be retained in accordance with the Records Management Code of Practice[4]. You can check the schedule here[5]. Has provision been made to ensure you are able to accommodate this? If No, describe how the data will be managed.	Data is kept for the duration of the contract and will be securely deleted once the customer's data has been sent to the customer (following written confirmation).
	If data is being processed by a third party, how will we ensure data is deleted when required? Appropriate evidence would be an embedded copy of the contract or agreement containing this detail	As above.
	What will happen to the data at the end of the project/activity or end of contract with a third party? Will it be returned or deleted and how will this be done? Most contracts specify what happens to data at the end of contract. If this is not subject to contract, how will you ensure the data held by any third party is deleted? Embed extract of contract as necessary with highlighted sections.	As above.

Q16	**Have the personal/special categories of data been minimised?**	
	Please explain why a smaller amount of data cannot be used and explain	The minimum data sets for identification will be used in all CoreStream modules.

[4] https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8647

[5] https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/#appendix-ii-retention-schedule

	why all the data fields are necessary to achieve the objective. You are required to minimise the amount and level detail of any data set. For example, dates of birth should not be used where age would provide sufficient information to achieve the project aim.	All of the special category data fields have been highlighted, this is due to the Trust does not have control of the information that is being provided within a FOI/SAR request.
	How will you prevent function creep?	Scope is tightly limited to the items agreed to within the proposal.
	How will you ensure high standards of data quality?	All software is configured, peer reviewed, QA tested and then sent for UAT before it goes into production.

Q17	Is the data anonymised or pseudonymised in any way?	Anonymised	Pseudonymised
		□	□
	If the data is pseudonymised please describe how this has been done and the technical controls in place ie pseudonymised data provided to a third party and the 'key' for re-identification to be retained by the Trust.	Not applicable.	
	If the data is pseudonymised describe how the data will be transferred ie using HL7. ie Data will be sent using HL7. SSL (Security Socket Layer) and HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) are used in the encrypted transmission of data.	Not applicable.	
	Have you considered whether using anonymised/pseudonymised data is a suitable alternative, please explain how this has been considered and why it is not suitable?	Yes, using anonymised or pseudonymised data is not possible as it is necessary for effective processing of FOIs/SARs.	
	What steps have been taken to minimise the risk of re-identification of anonymised or pseudonymised data?	Not applicable.	

Step 3 – Data security

Q18	**Where will the data be stored?**			
	Will the data be stored on our servers or servers/cloud external to the Trust?			
	Internal	External	Server	Cloud*
	☐	☐	☒	☐
	If external, where will it be stored, will this be the UK, EU/EEA or elsewhere? Provide the location/country ie London, England		All data is hosted onshore in our primary data centre which is located outside of London. The backup data centre is located in London to ensure redundancy in the event of the primary data centre being unavailable.	
	If the data is processed outside of the EU/EEA, what safeguards will be in place?		N/A	
	If a supplier is used they must complete the supplier assurance framework below Supplier Assurance Framework TEMPLATE		Insert completed supplier assurance framework or state N/A if a supplier is not used	
	Will the storage be controlled by another party (not the supplier) such as a product/ platform supplier ie AWS, Google, Microsoft? Provide details		Data will reside on servers that are hosted by our partner, Lomart. Lomart is a partner rather than a sub-contractor and Corestream platform hosting is covered under the CoreStream contract (i.e., CoreStream takes full responsibility for hosting) therefore no additional contract is required between Lomart and our customers.	
	If the data is stored on the cloud the following assessment must be completed by the supplier Cloud Assessment.xlsx		N/A	
	If the data storage or processing is being done by a supplier, what certifications do they hold? When were they, and the proposed storage mechanism, subjected to an external penetration test and is a report available? (Please embed any documentary evidence)			

		Certificate	**External Penetration Test undertaken (date)**	**External Penetration Test Report**
	Cyber Essentials +/ Cyber Assessment Framework (CAF)	Cyber Essentials +: 6311c76c-fc11-4468-b3be-f7eb7d84e995 Expiry: 06/03/2024 Cyber Essentials: f6d8aa25-a968-4bae-b974-56cda6183665 Expiry: 06/03/24	18/09/23	We don’t supply this to clients for security reasons. The last report identified 0 critical, 0 high, 0 medium and 0 low priority findings. There were only 3 informational findings raised relating to a few outdated software instances.
	ISO 15489 Records Management	N/A		
	ISO 27001 Information Security Standards	Certificate number: 198722 Expiry: 12th September 2025		
	ISO/IEC 27701:2019 Ext to 27001/27002	N/A		
	ISO 27017 Cloud Services	N/A		
	ISO 27018 PII in public clouds	N/A		
	Digital Technology Assessment Criteria for Health and Social Care (DTAC)	N/A		
	ISO 9001 Quality Management Systems	N/A		

	Other, please specify	N/A		
	If a supplier is used are they registered with the ICO. Check the register[6] and provide the certificate number	Yes	No	
		☒	☐	
		Registration reference: ZA154741		
	If a supplier is used, have they completed the Data Security and Protection Toolkit, search the register here[7]	Yes	No	N/A
		☐	☐	☐
	If yes, complete the following	Organisation code	Status	Date Published
			Choose an item.	

Q19	**How will this data be secured during storage and when being moved?**			
	Will it be encrypted when stored and/or moved, if so what type of encryption will be employed?	All data is encrypted in transit and at rest. CoreStream utilise SHA2 (RSA), recognised as one of the strongest. Information is transported via HTTPS with TLS 1.2/AES 256 bit for data in transit		
	Will it be on a server protected by firewall and network intrusion detection?	CoreStream has firewalls and IDS in place.		
	What technical controls are in place to prevent hacking of the data by unauthorised persons?	Vulnerability scanning, Intrusion Detection System, firewalls, anti-virus software, access controls.		
	When being moved will it be secured through encrypted file transfer, secure transmission through SLL/TLS/SHS, please explain the specific technical standards that will apply?	CoreStream utilise SHA2 (RSA), recognised as one of the strongest. Information is transported via HTTPS with TLS 1.2/AES 256 bit for data in transit		
	Do you have a business continuity plan for the information?	Yes – last updated and tested in August 2023.		
	What types of backups are undertaken i.e. full, differential or incremental?	Full	Differential	Incremental
		☒	☐	☐

[6] https://ico.org.uk/ESDWebPages/Search
[7] https://www.dsptoolkit.nhs.uk/OrganisationSearch

Q20	Who will have access to this data and how will this access be controlled?		
	Will the data be kept on a system that is password controlled, what is the password length and how often does it have to be changed? Who will administer these access controls?	All systems are password controlled and access is on a need-to-know basis. Passwords must be a minimum of 12 characters and contain upper case, lower case, numbers, and special characters. Only CoreStream system administrators (of which there are 3 per client instance) can provide access to client sites. This goes through an approval process and accounts are then deactivated when no longer required.	
	Is there an ability to audit access to the information? Can the supplier audit our data?	Yes – audit history is available throughout the platform. CoreStream cannot audit the Trust's system without gaining consent. The only instances where CoreStream will require access to the Trust's platform is when issues are raised via Support that require investigating and fixing.	
	What other security measures are in place, such as physical security, smartcard, Active Directory, multiple factor authentication?	Physical security within the data centre (where servers are hosted) and CoreStream's office, SSO, MFA, segregation of duties.	
	Is training available to staff for the new system?	Yes	No
		☒	☐

Q21	If you are using devices such as laptops to access data, how are these secured and managed?
	Via passwords

Q22	Is this data an attractive target for criminals and hackers; does it contain information that may be used for identity/financial fraud or reveal a person possibly being vulnerable to exploitation?	
	Yes ☒ Rate its attractiveness from 0 to 10 below. https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime Choose an item.	No ☐

	If this is a risk describe how you will manage it in stage 8.	

Step 4 – Data use and sharing

Q23	**Will this data be shared with anyone else?**	
	If yes, explain who these other parties are and why the data is being shared?	No

Q24	**Are other people processing this data?**	
	If a third party such as a company is storing or otherwise managing or using our data, please explain what they doing and why they are doing it?	CoreStream outsources its hosting to Iomart Plc. CoreStream's hosting partner, Iomart, are the most accredited UK cloud hosting company. For a full list of accreditations please go to: https://www.iomart.com/about-iomart/accreditations/ All datacenters conform to Tier 3 TIA standards for redundancy and resilience. Iomart and CoreStream have both attained the ISO27001 accreditation for technology development and hosting security. Iomart are one of the only UK hosting providers to be PAN Government IL2 and IL3 and they are able to host public sector data to classified levels.
	If we are using a third-party product that requires maintenance where they access our networks, explain how this will be managed (will they remotely connect, how will this access be managed).	N/A
	Is there a process in place to remove personal data if data subject refuses/removes consent? ie The right to restrict processing/the right to object - People can request the use of their data to be restricted in certain circumstances. These will be considered on a case-by-case basis.	The SOP would remain the same for processing FOIs and SARs.
	Are arrangements in place for recognising and responding to requests for access to personal data?	The Trust has a policy and procedure for responding to subject access requests. Further information for patients on how to access their records is here: Sherwood Forest Hospitals (sfh-tr.nhs.uk)

Q25	**Describe the data flows**	
	Please complete the data flow template below to detail how the data is collected, moved and used? IG - Flow Maps.xlsm	Attached.
	Are there security or data protection concerns in any of the data flow stages you identify? If so, please indicate where and what steps you taking to reduce these risk?	N/A

Step 5 – Processing by or with a supplier/third party

Q26	**If you are using a supplier or organisation to process, store or otherwise interact with this data, if not answer N/A**	
	What is the arrangement between the Trust and the supplier/third party concerned?	A contract to provide Information Governance software to SFH.
	What activities will the supplier/third party carry out i.e. storage, transport, processing of data on their platform	Supply, maintenance, storage and support of the Information Governance platform.
Q27	What steps or measures will you put in place to manage these risks? What measures will you take to ensure processors comply? PLEASE ATTACH COPIES/ RELEVANT SECTIONS OF ANY CONTRACT/ AGREEMENT.	Corestream IG System U4 432 Final

Step 6 – Consultation

Q28	Consider how to consult with those who have an interest in this project	
	Describe when and how you will seek individuals' views or justify why it's not appropriate to do so. ie do we need wider public engagement.	The DPIA will be forwarded to the Information Governance Working Group for wider stakeholder engagement. Public engagement is not required it is a changing of internal process and supplier.
	Who else do you need to involve within the Trust? ie Digital Innovations Approval Group (DIAG).	Corestream was taken to DIAG on 21/02/2023. Will got to the Information Governance Group for review and comment. Sign off via the Caldicott Guardian & DPO
	Do you need to ask the data processors (supplier) to assist?	Not required.
	Do you plan to consult information security experts, or any other experts?	Yes, NHIS will review the security assessments.

Step 7 – Lawful basis

Q29	**What is your lawful basis for processing personal data? Select all that apply**	
	a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes. **Please note, do not use this if it is for direct care, (e) maybe more appropriate**	□
	b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract	□
	c) processing is necessary for compliance with a legal obligation to which the controller is subject	☒
	d) processing is necessary in order to protect the vital interests of the data subject or of another natural person	□
	e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller	□

Q30	**What is your lawful basis for processing special categories of personal data? Select all that apply**	
	a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes. **Please note, do not use this if it is for direct care, (h) and/or (i) maybe more appropriate**	☒
	b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment	□
	c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent	□
	e) processing relates to personal data which are manifestly made public by the data subject	□
	h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services	☒

	i) processing is necessary for reasons of substantial public interest, ie public health, such as protecting against serious cross-border threats to health	□
	j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purpose	□

Stage 8 – Risk Template

For advice on completing this Risk Template please contact the Risk & Assurance Manager on x6326

Completed by: Sophie Lis	Role:	Date completed:

Guidance notes:

Confidentiality - Are there any risks to the confidentiality of personal data? Do staff have a legitimate relationship in order to process personal data? Is personal data disclosed to people who do not require it?

Integrity - Systems must be designed so that the input and management of information is not prone to human error and that the flow of information does not result in loss or alteration. Data should be complete and accurate and not tampered with during or after submission. Ensuring that during the process of transmission data integrity is maintained.

Availability - System design must include appropriate access controls and checks, so that the information in the system has consistency, accuracy, can be trusted as correct and can be relied on when providing healthcare. Data is available and delivered to the right person, at the time when it is needed and that there is accessibility to systems at all times. Having safeguards in place for power outages, natural disasters, hardware failures and systems upgrades.

Examples of risks that are common in projects is included below. Please amend/delete as necessary.

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Data subject provides more data that is required to carry out the task of the request. Data subjects not using the standard forms. More data being processed than needed. Leading to IG breach and potential regulator action.	Forms are provided on the Trust website for data subjects to complete when making an FOI or SAR request, which will only require them to complete the mandatory fields.	2	2	4	If the risk is not controlled appropriately then the data subject will potentially provide sensitive data which is not required.	2	2	4	Ensuring that there are sufficient security controls in place (MFA, Single Sign On, complex passwords) to ensure that sensitive data is adequately protected.
Data subject information sent to the wrong requestor. Human error. Disclosed in error.	Multifactor checking when responding to requests. Name Email Reference number	2	2	4	If the risk is not controlled appropriately then the data subject will receive the wrong information which is a data breach.	2	2	4	The 'final review' workflow stage has been designed to independently check for errors before data is

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Leading to IG breach and potential regulator action.				🟩				🟩	disclosed to the data subject.
Loss of system access due to connection failure or server failure via 3rd party supplier. This could result in the service being disrupted or unavailable. The consequences of this could be enforcement action and reputational damage to the Trust	Full system back-up processes and ISO 27001 accreditation in place Business continuity plan in place Regular updates from supplier to advise users of any planned updates and a process is in place to contact all main users for support during any unplanned downtime.	2	2	4	If the risk is not controlled appropriately then outages may occur.	2	2	4	**Redundancy factored into data centres, plus servers are continually monitored and outages reported and fixed within SLA response times.**

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Loss of system data due to connection failure or server failure by third party supplier. This could result in the service being disrupted or unavailable. The consequences of this could be enforcement action and reputational damage to the Trust	Full system back-up processes and ISO 27001, 27017 and 27018 accreditations in place Business continuity plan in place	2	2	4	As above.	2	2	4	As above.
If the system is not recorded on the information asset register, the system may not be brought back online in	In the Trust we have a business continuity plan if the service was unavailable. The department would default back to the current practice.	2	2	4		2	1	**2**	Corestream will need to be added to the divisional information asset register and the data flows mapped and

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
response to a cyber attack. The consequences of this could be enforcement action and reputational damage to the Trust.				🟩				🟩	recorded as part of the annual IAO returns to the SIRO
Data is accessed inappropriately due to lack of access controls. Movers and leavers access not removed. Data is inappropriately processed and/or disclosed, leading to IG breach and potential regulator action.	Username and password controls in place. Access is managed within the IG Team team. Account Management and access procedure to be audited on a regular basis. Appropriate access according to role. IG Training in place.	2	2	4		2	2	**4**	Single Sign On will prevent users from inappropriately accessing the platform after they have left the Trust, as once their Active Directory account has been deactivated they will no longer be able to authenticate and

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
									access CoreStream.
Adequate data processing agreements with relevant data processors, to be established and agreed to protect Sherwood Forest Data. If these were not in place there is the risk of data breaches. The consequences of this could be enforcement action and reputational damage to the Trust.	A contract and data processing agreement between CoreStream and the Trust is in place developed. Separate processing agreements where necessary will be in place with additional providers of data.	3	1	3					Contract covers data processing and GDPR.

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Personal data not being encrypted both/either in transit or at rest, leading to IG breach and potential regulator action.	Web-upload technology which automatically compresses all images/data before transit and transmits the above over HTTPS/TLS1.3 encrypted connection.	3	1	3					All data is encrypted in transit and at rest by default.

Risk Scoring Matrix.pdf

Step 8 – Legal compliance

To be amended by Information Governance from the responses provided in the previous stages.

UK General Data Protection Regulation 2018	Compliance
Principle 1 – Personal data shall be processed fairly and lawfully and, in a transparent manner.	Lawfulness • We have identified an appropriate lawful basis (or bases) for our processing. • We are processing special category data and have identified a condition for processing this type of data. • We don't do anything generally unlawful with personal data. Fairness • We have considered how the processing may affect the individuals concerned and can justify any adverse impact. • We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified. • We do not deceive or mislead people when we collect their personal data. Transparency • We are open and honest and comply with the transparency obligations of the right to be informed.
Principle 2 – Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.	• We have clearly identified our purpose or purposes for processing. • We have documented those purposes. • We include details of our purposes in our privacy information for individuals. • We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.

	• If we plan to use personal data for a new purpose other than a legal obligation or function set out in law, we check that this is compatible with our original purpose, or we get specific consent for the new purpose.
Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.	• We only collect personal data we actually need for our specified purposes. • We have sufficient personal data to properly fulfil those purposes. • We periodically review the data we hold and delete anything we don't need.
Principle 4 – Personal data shall be Accurate and, where necessary, kept up to date, having regard to the purposes for which they are processed, are erased or rectified without delay.	• We ensure the accuracy of any personal data we create. • We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data. • We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary. • If we need to keep a record of a mistake, we clearly identify it as a mistake. • Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts. • We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data. • As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data
Principle 5 – Kept no longer than is necessary.	• We know what personal data we hold and why we need it. • We carefully consider and can justify how long we keep personal data. • We have a policy with standard retention periods, however due to three Inquiries including the Goddard Inquiry, no destruction or deletion of patient records is to take place until further notice. • We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

Principle 6 – Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.	• We undertake an analysis of the risks presented by our processing and use this to assess the appropriate level of security we need to put in place. • When deciding what measures to implement, we take account of the state of the art and costs of implementation. • We have an information security policy and take steps to make sure the policy is implemented. • When deciding what measures to implement, we take account of the state of the art and costs of implementation. • We make sure that we regularly review our information security policies and measures and, where necessary, improve them. • We have assessed what we need to do by considering the security outcomes we want to achieve. • We have put in place technical controls such as those specified by established frameworks like Cyber Essentials. • We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process. • We use encryption and/or pseudonymisation where it is appropriate to do so. • We understand the requirements of confidentiality, integrity and availability for the personal data we process. • We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process. • We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. • Where appropriate, we implement measures that adhere to an approved code of conduct or certification mechanism. • We ensure that any data processor we use also implements appropriate technical and organisational measures.

Principle 7 – Accountability principle	• We take responsibility for complying with the UK GDPR, at the highest management level and throughout our organisation. • We keep evidence of the steps we take to comply with the UK GDPR. • We put in place appropriate technical and organisational measures, such as: ☐ Adopting and implementing data protection policies (where proportionate). ☐ taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations. ☐ putting written contracts in place with organisations that process personal data on our behalf. ☐ maintaining documentation of our processing activities. ☐ implementing appropriate security measures. ☐ recording and, where necessary, reporting personal data breaches. ☐ carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests. ☐ appointed a data protection officer; and ☐ adhering to relevant codes of conduct and signing up to certification schemes (where possible). ☐ We review and update our accountability measures at appropriate intervals.

Step 9 - Assessment Summary

To be completed by Information Governance.

Outcome of Data Protection Impact Assessment	
Project is not recommended to proceed, as significant risks have been identified.	☐
Project to proceed once identified risks have been mitigated as agreed.	☐
Project has met required legislative compliance and poses no significant risks. No further action required.	☒

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks	
Legislative Compliance:	Article 6(1)(c) processing is necessary for compliance with a legal obligation to which the controller is subject. Article 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity) Article 9(2)(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where [F1domestic law provides] that the prohibition referred to in paragraph 1 may not be lifted by the data subject.
Summary of Risks	Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management.
Identified risks	
The risk	**Mitigation**
Loss of system access	Full system back-up process in place
Loss of system data	Full system back-up process in place
Data is accessed inappropriately	individual username and passwords are provided. There is a risk of unauthorised

	access due to the system being unable to report on users that have accessed individual patient records
Adequate data processing agreements with relevant data processors	Agreements in place.

Step 10 - Recommendations for Action

Summary of recommendations (amend/delete as necessary)		
Recommendations	**Recommendations**	**Agreed deadline for action**
Information Asset Administrators to ensure Corestream is added to the information asset register and data flows are mapped and recorded.	IAO/IAA	
Ensure business continuity plans are in place.	IAO/IAA	
Account management Standard Operating Procedure generated and implemented, routine audit to take place.	IAO/IAA	

Step 11 - Project signoff

	Name	Job Title	Date
Information Asset Owner*	Jacquie Widdowson	Divisional General Manager	29.03.2024
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	29.03.2024
Senior Information Risk Owner	Sally Brook Shanahan	Director of Corporate Affairs	09.04.2024
Caldicott Guardian	David Selwyn	Medical Director	09.04.2024
Chief Digital Information Officer	Paul Moore	Acting Chief Digital Information Officer	02.03.2024
Patient safety[8]			

The Data Protection Impact Assessment must be reviewed and approved by the Information Asset Owner, Data Protection Officer, Senior Information Risk Owner and Caldicott Guardian.   Approval does not close the data protection risks related to this project.

*It is important that the risks and the original scope of the project are reviewed on a regular basis to ensure any new confidentiality, integrity or availability risks are identified, documented, and mitigated wherever possible. All amendments must be approved following the approvals process.

[8] DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital