Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

Data Protection Impact Assessment

Title	Ref number
EDGE Local Portfolio Management System	EDGE 2021

Introduction

A Data Protection Impact Assessment enables Sherwood Forest Hospitals NHS Foundation Trust (the Trust) to meet its legal/compliance obligations with the Data Protection Act 2018 and the General Data Protection Regulation 2016.

The Data Protection Impact Assessment (DPIA) ensures the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed, as required under ISO/IEC: 27001:2017. It is important that the DPIA is part of and integrated with the organisation's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. The process identifies and allows issues to be mitigated at an early stage of implementation/change thereby reducing associated costs and damage to reputation. Data Protection Impact Assessment are an integral part of the "privacy by design" approach as identified by the Information Commissioner's Office.

Document Completion

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.

This document, and the privacy risks, actions and recommendations identified within it, will be accepted in the Project Sign Off (page 3). The project will need to signed off by the Information Asset Owner, Information Governance/Data Protection Officer and a customer representative (if applicable) and through the appropriate governance structure of the implementing organisation. Sign off and acceptance of the document does not close the privacy risks related to this project. It is important that the risks are revisited during the life of the project and any additional privacy risks identified are appropriately reviewed and mitigated.

PLEASE NOTE:
The Information Asset Owner (implementer) undertaking the Data Protection Impact Assessment has a responsibility to ensure that Patient Safety, Technical Security and Quality Impact Assessments are considered, in line with the Trust procedures.
Assessment Process Stages

Activity	IAO	Governance
Complete Title Bar and include Ref Number	Alison Steel	
Complete Project Details and check the Initial Screening Questions	Alison Steel	

Complete Stage 1 – Introductory meeting and review Initial Screening Questions and follow up questions to determine if a Stage 2 – DPIA (Full) is to be undertaken	Alison Steel Alison Steel	
Initial Screening Questions to be formally written up and Introductory Meeting to be formally recorded	N/A Already in use	

If a Data Protection Impact Assessment **IS NOT** required		
Activity	**IAO**	**Governance**
Complete Assessment Summary & Recommendations for Action	N/A	
Assessment to be passed to Implementer	N/A	
Ensure Sign Off is completed	N/A	
Assessment shared with customer if appropriate	N/A	
Assessment to be kept with project documentation copy to Information Governance	N/A	

OR

If a Data Protection Impact Assessment **IS** required		
Activity	**Implementer**	**Governance**
Complete Stage 2 – Data Protection Impact Assessment (Full)	Alison Steel	
Complete Stage - 3 Work Flow Mapping	Alison Steel	
Complete Stage - 4 Identified Risks and Mitigating Action	Alison Steel	
Complete Stage – 5 Legal Compliance	Alison Steel	
Complete Assessment Summary & Recommendations for Action		
Closure meeting for final agreement		
Ensure Sign Off is completed		
Assessment shared with customer if appropriate		
Assessment to be kept with project documentation copy to Information Governance		

This document is intended to be completed by the Trust and external organisations the *Governance* section will be completed by the IG Team with support from the relevant NHIS specialist teams as applicable.

Project Details

Project Title:	**EDGE Local Portfolio Management System**

Project Description: Describe in sufficient detail for the proposal to be understood
EDGE is a local portfolio management system provided by the Clinical Research Network (CRN). It is an online/web-based database with username/password access (granted by administrator at the trust) that records all trial activity, this includes active and inactive trial data, participant data and staff data. The database exists on 2 levels, local and national. Data accessed by persons outside of the Trust is statistical and not patient identifiable. Data accessed by persons within the Trust can be identifiable if required, this is controlled by an administrator.

Overview of the proposal: What the project aims to achieve
EDGE provides a central database for storing valuable research and recruitment data. Data held needs to be identifiable by limited persons in the Trust to use the project (EDGE) to its full potential.

Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in DPIA assessment (Include Email Address):	Alison Steel, Head of Research and Innovation Terri-Ann Sewell, Research Nurse Donna Sowter, Research Support Facilitator / Information Manager

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Alison Steel	Head of R&I	Sherwood Forest Hospitals NHS FT	2nd March 2021
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	3rd August 2022
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	6th June 2022
Senior Information Risk Owner	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	3rd August 2022
Caldicott Guardian	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	5th August 2022
Chief Digital Information Officer	Richard Walker	Chief Digital Information Officer	Sherwood Forest Hospitals NHS Foundation Trust	5th August 2022

Assessment Summary

To be completed by Information Governance

Outcome of Data Protection Impact Assessment:	
1. Project/Implementation is recommended **NOT** to proceed, as significant corporate/customer risks have been identified.	☐

2. Project/Implementation to proceed once identified risks have been mitigated as agreed.	☒
3. Project/Implementation has met required legislative compliance and poses not significant risks. No further action required.	☐

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks:

Summary:

Legislative Compliance:

Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

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)(i) allows processing for "ensuring high standards of quality and safety of health care." – which would cover research, audit, service improvement and addressing public health/inequalities

Summary of Risks:
Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management.

Risks

1. Loss of system access - Full system back-up process in place
2. Loss of system data - Full system back-up process in place
3. Leavers' access not removed – Trust EDGE administrator terminates access in real time
4. Business continuity plans is currently under review - Not having up to date plans could lead to access to data problems or service delivery problems.
5. EDGE will need to be added to the divisional information asset register and the data flows remapped and recorded as part of the annual IAO returns to the SIRO
6. Data is accessed inappropriately – individual username and passwords are provided and the systems defaults for changes every 180 days

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	**Recommendation Owner:**	**Agreed Deadline for action:**
Information Asset Administrators to ensure EDGE is added to the information asset register and revised data flows are mapped and recorded as part of the annual submissions to IG	IAA	31st August 2022
Ensure business continuity plans are in place	IAA	31st August 2022
Account management Standard Operating Procedure generated and implemented,	IAA	31st August 2022
Routine audit to take place. The audit is part of the leavers checklist to remove access to EDGE and as and when someone leaves the department. The audit tends to take place in real time on more of an adhoc basis but will take place quarterly if there are no leavers.	IAA	31· August 2022

Stage 1 – Initial Screening Questions

Answering "**Yes**" to a screening questions below represents a potential IG risk factor that may have to be further analysed to ensure those risks are identified, assessed and fully mitigated. The decision to undertake a full DPIA will be undertaken on a case-by-case basis by IG.

Q	Screening question	Y/N	Justification for response
1	Will the project involve the collection of information about individuals?	Y	Patient initials, DOB, D number/NHS Number and trial enrolled into will be collected.
2	Will the project compel individuals to provide information about themselves?	N	
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	N	
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N	
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	Reports taken 2 weekly to assess recruitment data, as well as Adhoc requests. Monthly IG checks are performed to ensure access requirements are correct
6	Are there security arrangements in place while the information is held?	Y	Username and Password required; access given by IAA. Password management is set as default at 180 days • A minimum of 8 or more characters • At least 1 uppercase Letter • At least lowercase Letter • At least 1 number or symbol EDGE utilises API's with password breach databases to identify the use of passwords which are insecure. Any password identified as insecure will be

Q	Screening question	Y/N	Justification for response
			rejected by the system. 3 failed password attempts before user account is locked.
7	Does the project involve using new technology to the organisation?	N	
8	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	N	
If you have answered "Yes" to any of the questions numbered 1-8 please proceed and complete stage 2.			
9	Is a Patient Safety Review required?	N	22.04.2022 – NHIS have reviewed and advised that a patient safety case is not required.
10	Is a Quality Impact/Technical Security Review required?	Y	Microsoft is ISO27001 compliant https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001 https://docs.microsoft.com/en-gb/azure/compliance/

Please ensure that on completion this is returned to Information Governance lead to agree how to proceed.

Stage 2 – Data Protection Impact Assessment

2.1	What is the change					
	New purpose?	☐	Revised/changed?	☒	Other?	☒
	If Other please specify.		In use since 2015, previous PIA submitted			

2.2.1	What data will be processed?					
	Personal Data:					
	Forename	☒	Surname	☒	Age	☐
	DOB	☒	Gender	☒	Address	☐
	Post Code	☐	NHS No	☒	Hospital No	☒
	Other unique identifier (please specify)					
	Sensitive Personal Data (special categories):					
	Children **(via d.o.b only)**					☒
	Vulnerable groups					☐
	Racial or ethnic origin					☐
	Political opinion					☐
	Religious Belief					☐
	Trade Union Membership					☐
	Physical or mental health or condition **(not documented on data collection plan, however can be related to the nature of the study)**					☒
	Sexual Health					☐
	Criminal offence data					☐
	Other data (please specify)					

2.2.2	Is the data?					
	Identifiable?	☐	Pseudonymised?	☒	Anonymised?	☐

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	To ID patients taking part in research, to avoid duplication

2.3.1	How will you collect, use, store and delete data?
	Collected with explicit consent of the patient following a detailed discussion and information provided. Used to ID recruits to each trial.
2.3.2	What is the source of the data? (i.e. from data subject, system or other third party)
	Data subject, Dragon Medical, CareFlow EPR and case notes
2.3.3	How much data will you be collecting and using?
	As detailed in 2.2.1
2.3.4	How often? (for example monthly, weekly)
	Data is collected and recorded ad-hoc on a daily basis
2.3.5	How long will you keep it? https://www.sfh-tr.nhs.uk/media/12002/isp-101-records-management-code-of-practice-2021.pdf
	Indefinitely. Recruitment figures are linked to a national database Central portfolio management system. Local portfolio management system (EDGE) feeds top level data into this, i.e. recruitment data only. Only trust level access granted by IAA gives access to patient identifiable data.
2.3.6	Where will the data be stored? i.e. Medway, Shared Drive, offsite storage
	Microsoft Azure UK Data Centre South and on Trust servers
2.3.7	How many individuals are affected?
	Unknown – Any research participant
2.3.8	What geographical area does it cover?
	Local / UK

2.4	Who are the Organisations involved in processing (sharing) the data?	
	Organisations Name	Data Controller or Data Processor *The **Data Controller** is 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.* *The **Data Processor**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.*
	University of Southampton and Sherwood Forest Hospitals NHS Foundation Trust	Data Controller and Processor – the Trust control their own data but also processes data for the overall Controller University of Southampton.
	University of Southampton	Data Processor
	Microsoft Azure	3rd party hosting provider

2.5	If we have identified a supplier in 2.4, the following questions for 2.5 and 2.6 will need to be answered by the supplier and the Trust	
		If yes the third party will need to complete the following assessment. This will need to be provided in addition to the completion of this proforma. An example of a completed assessment is also provided below NHIS - Supplier Assurance Framework Supplier Assurance Framework - Example
		As the Trust extracts and uploads the data to the database, there is no access to existing Trust network or systems. Microsoft is ISO27001 compliant https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001
2.5.1	Please describe access and controls in place https://www.sfh-tr.nhs.uk/media/12007/ig-012-account-management-and-access-policy-2021.pdf	

	 Account ManagementSOP Ten			
	User account management is the responsibility of the Trust EDGE Administrator Privileged account management is the responsibility of the Trust EDGE Administrator			
2.5.2	Please provide a copy of the contract in place			
	Contract is via University of Southampton and the CRN.  Xerox Scan_08042022095743			
2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?			
	Yes, data will only be retained externally for the duration of the contract			
2.5.4	Is the supplier registered with the ICO? Please check the register	Yes	No	
		Z6801020		
2.5.5	Has the supplier received ICO Enforcement? Please check the register	Yes	No	
			x	
2.5.6	Has the supplier received ICO Decision Notice? Please check the register	Yes	No	
		x10 in relation to Freedom of Information Act		
2.5.7	Has the supplier received an ICO Audit? Please check the register	Yes	No	
			x	
2.5.8	Has the supplier completed a Data Security and Protection Toolkit, please check the register and	Completed: Yes/No	Date submitted	Standard Met/Not Met
		Yes	27th June 2022	Standards Met

	provide the following details			
2.5.9	Can the supplier demonstrate compliance with any of the following standards? If YES please provide further information e.g. date achieved and a copy of the certificates			
		Yes		No
	Cyber Essentials Plus			X IASME-CE-003619 CE only
	ISO 15489 Records Management			x
	ISO 27001 Information Security Standards	Microsoft https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001		
	ISO 9001 Quality Management Systems	Microsoft https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-iso-9001?toc=/compliance/regulatory/toc.json&bc=/compliance/regulatory/breadcrumb/toc.json		
2.5.10	Is the data held outside of the UK ie Europe, USA, Ireland? If yes please include the country			
	Yes		No	
			No, UK South	
	If yes we need to seek assurance that the data will continue to flow post Brexit 31.12.2020, provide further detail below from the supplier			
	Not applicable			
2.6	Will this information be shared outside the organisations listed above?			
	Y/N	if answered **Yes** please describe organisation/s and geographic location		
	N			

2.7	Does the work involve employing contractors external to the Organisation?					
	Y/N	If **Yes**, provide a copy of the confidentiality agreement or contract?				
	N					
2.8	Has a data flow mapping exercise been undertaken?					
	Y/N	If **Yes**, please provide a copy here. Have the information flows and assets that are identified within this DPIA been added to your departmental information flow map and asset register? If **No**, please complete – Section 3				
	N	The Trust will need to remap the flow of data for this service as part of the annual submission to IG. Added as a recommendation to the DPIA.				
2.9	What format is the data?					
	Electronic	☒	Paper	☐	Other (Please describe)	Click here to enter text.

2.10	Is there an ability to audit access to the information?	
	Y/N	Please describe if answered **Yes.** If **NO** what contingencies are in place to prevent misuse?
	Y	Audit log on EDGE database. The EDGE audit log captures the following items · Time and Date of action · User performing the action · The type of action and context performed · Data change / action The type of action which the audit log will capture are: Create / Delete / Insert / Merge / Update / Reorder. Any End-User who has been provided with Administrative permissions can access and query the audit log.

2.11	Does the system involve new links with personal data held in other systems or have existing links been significantly changed?	
	Y/N	Please describe if answered **Yes**

	N	

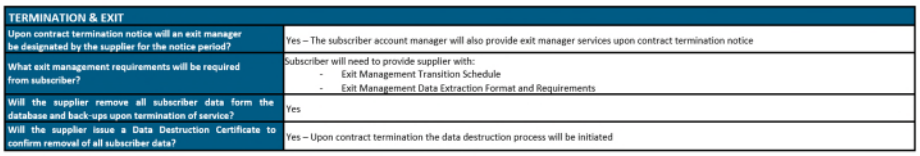
2.12	How will the information be kept up to date and checked for accuracy and completeness? (data quality) How will you ensure data minimisation?	
	Regular reports produced by IAA	
2.13	Who will have access to the information? (list individuals or staff groups)	
	Those employed by Research & Innovation and granted access to the system by the IAA only	
2.14	What security measures have been implemented to secure access?	
	Active Directory (Window's username and password)	☒
	Username and password	☒
	Smartcard	☐
	Key locked filing cabinet/room	☐
	Hard/soft Token (VPN) Access	☐
	Restricted Access to Network Files (shared drive)	☐
	Has information been anonymised?	☐
	Has information been pseudonymised?	☐
	Is information fully identifiable?	☒
	Other (provide detail below)	☒
	Access is removed as part of the leavers checklist developed by IAA's. Password changed by default every 180 days) • A minimum of 8 or more characters • At least 1 uppercase Letter • At least lowercase Letter • At least 1 number or symbol	

	EDGE utilises API's with password breach databases to identify the use of passwords which are insecure. Any password identified as insecure will be rejected by the system. 3 failed password attempts before user account is locked. Microsoft https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001  A+-+EDGE+Sample+Security+Questionnair

2.15	Will the data be stored on Trust servers			
	Yes	No		
		x		
2.16	Please state by which method the information will be transferred?			
	Email (not NHS.net)	☐	NHS.net	☐
	Website Access (internet or intranet)	☒	Wireless Network (Wi-Fi)	☐
	Secure Courier	☐	Staff delivered by hand	☐
	Post (internal)	☐	Post (external)	☐
	Telephone	☐	SMS	☐
	Fax	☐	Other (please specify below)	☐
	N/A – No identifiable data is transferred. Data will be uploaded via secure portal. User can only connect to secure portal from Trust network (or via VPN connection).			
2.17	Are disaster recovery and business contingency plans in place for the information? What types of backups are undertaken i.e. full, differential or incremental?			

	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	Web-based system and all back-up/recovery/contingency plans are provided by Microsoft Azure. No identifiable data is shared with them. In the Trust we have a business continuity plan if the service was unavailable. Yes – Disaster Recovery is managed through Cancom services management. Full back up every 24 hours. Differential back up every 30 minutes. An automated test restore from the backup database is performed monthly. A manual back-up and restore is performed annually. Back-ups are sent to co-located fail overs facilities every 24 hours. Recovery Time Objective: 24 Hours Recovery Point Objective: 30 Minutes
2.18	Has staff training been proposed or undertaken and did this include confidentiality and security topics areas?	
	Y/N	Please describe if answered **Yes**
	Y	All those given access to the EDGE database are required to receive training by the IAA where confidentiality and details of what should and should not be recorded are explicit. It is always stressed that identifiable data should be kept to a minimum and for purpose only.
2.19	Will reports be produced?	
	Will reports contain personal/sensitive personal or business confidential information?	Y
	Who will be able to run reports?	IAA
	Who will receive the reports and will they be published?	Those delegated to the trial

<table>
<tr><td></td><td colspan="2"></td><td>and with permission</td></tr>
<tr><td rowspan="3">2.20</td><td colspan="3">If this new/revised function should stop, are there plans in place for how the information will be retained / archived/ transferred or disposed of?</td></tr>
<tr><td>Y/N</td><td colspan="2">Please describe if answered Yes. Please state why not if response is No.</td></tr>
<tr><td>Y</td><td colspan="2">A copy of the trial consent and participant information sheet (PIS) as well as nursing notes will be in the patient’s medical records, along with being retained in the study site file.

 
<table>
<tr><th colspan="2">TERMINATION & EXIT</th></tr>
<tr><td>Upon contract termination notice will an exit manager be designated by the supplier for the notice period?</td><td>Yes – The subscriber account manager will also provide exit manager services upon contract termination notice</td></tr>
<tr><td>What exit management requirements will be required from subscriber?</td><td>Subscriber will need to provide supplier with:
- Exit Management Transition Schedule
- Exit Management Data Extraction Format and Requirements</td></tr>
<tr><td>Will the supplier remove all subscriber data form the database and back-ups upon termination of service?</td><td>Yes</td></tr>
<tr><td>Will the supplier issue a Data Destruction Certificate to confirm removal of all subscriber data?</td><td>Yes – Upon contract termination the data destruction process will be initiated</td></tr>
</table></td></tr>
<tr><td rowspan="4">2.21</td><td colspan="3">Is consent required for processing of personal data?</td></tr>
<tr><td>Y/N</td><td colspan="2">Please describe if answered Yes</td></tr>
<tr><td>Y</td><td colspan="2">Consent to the study given</td></tr>
<tr><td></td><td colspan="2">If No, list the reason for not gaining consent e.g. relying on an existing agreement, consent is implied, the project has s251 approval or other legal basis?</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
<tr><td rowspan="3">2.22</td><td colspan="3">Will individuals be informed about the proposed uses and share of their personal data?</td></tr>
<tr><td>Y/N</td><td colspan="2">Please describe if answered Yes. Please state why not if response is No.</td></tr>
<tr><td>Y</td><td colspan="2">How data is used is explained in the study participant information sheet and consent form. The Trust’s privacy notice is here https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/. The research team have reviewed the patient privacy notice and no more detail is required.

EDGE Privacy Policy - https://edgeclinical.com/privacy</td></tr>
</table>

2.23	Is there a process in place to remove personal data if data subject refuses/removes consent	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	Personal data for patients who refuse is not captured, anonymised data must remain for the purposes of research screening logs. When a patient removes consent it is of the understanding that their existing data will remain and so therefore removal not required
2.24	How much control will they have? Would they expect you to use their data in this way?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	How data is used in explained in the study participant information sheet and consent
2.25	Are arrangements in place for recognising and responding to requests for access to personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	N	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)
2.26	Who are the Information Asset Owner(s) and Administrator(s)?	
	IAO	Alison Steel
	IAA	Terri-Ann Sewell / Donna Sowter
	System Administrators	Donna Sowter / Melanie Greatorex
2.27	How is the data secured in transit? Eg encryption, port control number	
	Secure data transfer between systems (TLS 1.2). Encryption	

2.28	Has the impact to other NHIS systems/processes been considered and appropriate SBU's consulted and in particular technical security?	
	Y/N	Please describe if answered **Yes.** Please state what checks were undertaken if response is answered **No.**
	N	Not relevant as the Trust extracts and uploads the data to the web portal, there is no access or connection to existing Trust network or systems. 22.04.2022 – NHIS have reviewed and advised that a patient safety case is not required.
2.29	Are there any current issues of public concern that you should factor in?	
	Y/N	Please describe if answered **Yes.**
	N	
2.30	What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?	
	EDGE is used to maintain an overview of the Trust's Research Portfolio, it allows us to access opportunities for wider patient involvement in Research	
2.31	Consider how to consult with relevant stakeholders: • Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. • Who else do you need to involve within your organisation? • Do you need to ask your processors to assist?	
	EDGE was developed as part of a national research administration system by the University of Southampton.	

2.32	What is your lawful basis for processing? (please see Appendix 10 Information Sharing Protocol for further information). **Consent is usually the last basis to rely on** **Legal basis: patients** **Personal data i.e. name, address** 6(1)(a) the patient has given consent

	6(1)(c) necessary for legal obligations 6(1)(e) public interest or public duty 6(3) the above supported by Member State law (UK legislation as applicable to circumstances) **Sensitive personal data (special category)** 9(2)(a) the patient has given explicit consent 9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc.) 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). 9(2)(i) allows processing for "ensuring high standards of quality and safety of health care." – which would cover research, audit, service improvement and addressing public health/inequalities. 9(2)(j) (together with Article 89 and relevant recitals) relates to archiving, statistical analysis and research. **Legal basis: staff** – please review Appendix 10 Information Sharing Protocol for further information).
	6(1)(a) the patient has given consent 9(2)(a) the patient has given explicit consent
2.33	What information will you give individuals about the processing? (This information will be added to the Trust's Patient Privacy Notice and Staff Privacy Notice by the Information Governance Team)
	Study Participant Information Sheet, Consent Form, Verbal Instruction

2.34	What measures do you take to ensure processors comply?
	Identifiable data retained and processed by the Trust Research & Innovation staff only
2.35	How will you prevent function creep? Manage lifecycle of system/process
	Controlled by development team at University of Southampton

Stage - 3 Risk Template

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

Completed by: Donna Sowter Role: Research Support Facilitator / Information Manager Date completed: 21st April 2022
Gina Robinson, Information Security Officer updated 15th June 2022

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 access due to connection failure or server failure either via NHIS or 3rd party supplier. This could result in the service being disrupted or unavailable. The consequences of this could be patient harm, financial penalties and reputational damage to the Trust	Full system back-up processes and ISO 27001 accreditation in place	2	2	4	System back-up not present	2	2	4	Manual input, business continuity plan to be used
Loss of system data due to system failure and/or backup failure either via NHIS or 3rd party supplier. This could result in the service being disrupted or unavailable.	Full system back-up processes and ISO 27001 accreditation in place. All data entered onto the database is also available in paper form and where electronic it is saved to the shared drive.	3	1	3	System back-up not present	3	1	3	Manual input, business continuity plan to be used

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)**	
The consequences of this could be patient harm, financial penalties and reputational damage to the Trust									
Data is accessed inappropriately due to lack of access controls. Movers and leavers access not removed. Data is inappropriately processed and/or disclosed	Username and password controls in place. Account Management and access procedure to be completed. Appropriate access according to role. Segregation of duties. The Trust's EDGE administrator terminates access in real time	3	1	3	Ensure access is managed and leavers are actioned in real time. Routine audits.	3	1	**3**	Ensure access is managed and leavers are actioned in real time. Routine audits.
The system or service may not be able to operate due to system downtime or unavailability. Business continuity plans are not in place or available in each area.	Business Continuity plan for the EDGE system is currently under review	3	1	3	Business continuity plan in place.	3	1	**3**	Business continuity plan in place.
If the system is not recorded on the information asset register, the system may not be brought back online in response to a cyber attack	In the Trust we have a business continuity plan if the service was unavailable. The department would default back to the current practice and access the paper records and case notes	2	2	4	EDGE will need to be added to the divisional information asset register and the data flows remapped and recorded as part of the annual IAO returns to the SIRO	2	1	**2**	EDGE will need to be added to the divisional information asset register and the data flows remapped and recorded as part of the annual IAO returns to the SIRO

Risk Scoring Matrix.pdf

Stage – 4 Legal Compliance

Compliance to be determined by IG team from the responses provided in the previous stages, delete as appropriate:

Data Protection Act 2018	Compliance and Comment
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.
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 the Goddard Inquiry no destruction or deletion of patient records is to take place until further notice.
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.

	• We have an information security policy (or equivalent) and take steps to make sure the policy is implemented. We have put in place technical controls such as those specified by established frameworks like Cyber Essentials. • We use encryption. • 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. • 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.