

# Data Protection Impact Assessment

Title	Ref number
Sealed Envelope Electronic data Capture and randomisation system	October 2022

## 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**

<b>Activity</b>	<b>IAO</b>	<b>Governance</b>
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**

<b>Activity</b>	<b>Implementer</b>	<b>Governance</b>
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

<b>Project Title:</b>	<b>Sealed envelope electronic data capture system</b>
<b>Project Description: Describe in sufficient detail for the proposal to be understood</b>	
<p>Sealed envelope is an electronic data capture system and is a proven, reliable, centralised randomisation service owned by Clerkenwell Workshops in London and is supported by the NIHR. It is an online database with username/password access (granted by administrator) that records all trial data collected for a specific study and certain time points through the duration of the study and allows randomisation to take place securely. It is widely used across a number of studies nationally.</p> <p>Data collected includes active participant data such as consent date, demographics, investigation results, visit data and randomisation code generated by the system.</p>	
<b>Overview of the proposal: What the project aims to achieve</b>	
<p><a href="#">Sealed Envelope</a> Electronic data Capture system is a secure web application for building and managing online surveys, databases and collection of data form research studies.</p> <p>This system can be used to collect virtually any type of data, it is specifically geared to support online or offline data capture for research studies and operations. Using Sealed Envelopes stream-lined process for rapidly developing projects.</p> <p>Sealed Envelope provides user-friendly web-based case report forms, real-time data entry validation (e.g. for data types and range checks), audit trails, and the ability to set up a calendar to schedule and track critical study events such as blood-draws, participant visits, etc.</p>	
<b>Implementing Organisation:</b>	Sherwood Forest Hospitals NHS Foundation Trust
<b>Staff involved in DPIA assessment (Include Email Address):</b>	Alison Steel, Head of Research and Innovation Terri-Ann Sewell, Research Nurse

## Project Sign Off

	Name	Job Title	Organisation	Date
<b>Information Asset Owner</b>	Alison Steel	Head of R&I	Sherwood Forest Hospitals NHS FT	2 <sup>nd</sup> May 2023
<b>Data Protection Officer</b>	Jacque Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	9 <sup>th</sup> May 2023
<b>Information Governance</b>	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	26 <sup>th</sup> April 2023
<b>Senior Information Risk Owner</b>	Sally Brook Shanahan	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	2 <sup>nd</sup> June 2023
<b>Caldicott Guardian</b>	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	2 <sup>nd</sup> June 2023
<b>Chief Digital Information Officer</b>	Richard Walker	Chief Digital Information Officer	Sherwood Forest Hospitals NHS Foundation Trust	16 <sup>th</sup> May 2023

## Assessment Summary

To be completed by Information Governance

<b>Outcome of Data Protection Impact Assessment:</b>	
1. Project/Implementation is recommended <b>NOT</b> to proceed, as significant corporate/customer risks have been identified.	<input type="checkbox"/>
2. Project/Implementation to proceed once identified risks have been mitigated as agreed.	<input type="checkbox"/>
3. Project/Implementation has met required legislative compliance and poses not significant risks. No further action required.	<input checked="" type="checkbox"/>

<b>Summary of Data Protection Impact Assessment; including legislative compliance and identified risks:</b>
<p><b>Summary:</b></p> <p>Legislative Compliance:</p> <p>6(1)(a) the patient has given consent 9(2)(a) the patient has given explicit consent</p> <p><b>Summary of Risks:</b> Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management.</p> <p><b>Risks</b></p> <ol style="list-style-type: none"> <li>1. Loss of system access - Full system back-up process in place</li> <li>2. Loss of system data - Full system back-up process in place</li> <li>3. Data is accessed inappropriately – individual username and passwords are provided.</li> </ol>

## Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	Recommendation Owner:	Agreed Deadline for action:
Information Asset Administrators to ensure Sealed Envelope is added to the information asset register and data flows are mapped and recorded	IAO/IAA	31 <sup>st</sup> May 2023
Ensure business continuity plans are in place		31 <sup>st</sup> May 2023
The supplier to be informed of movers and leavers in the Trust, routine audit to take place		

## 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 and DOB.
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?	Y	Trial data collected. Not identifiable information. Identified via a trial number.
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?	Y	Research data collection.
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	Relevant data collected for Trial purposes only. No other data collected. Information collected form source documents. EG patient notes, results.
6	Are there security arrangements in place while the information is held?	Y	Username and Password required; access given by Sponsor. Password management is set as default at 180 days <ul style="list-style-type: none"> <li>• A minimum of 8 or more characters</li> <li>• At least 1 uppercase Letter</li> <li>• At least lowercase Letter</li> <li>• At least 1 number or symbol</li> </ul>
7	Does the project involve using new technology to the organisation?	N	



Q	Screening question	Y/N	Justification for response
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	
<b>Does the project include any of the following activities? (Mark all that apply and a description if answered 'Y')</b>			
9.1	Evaluation or scoring - including profiling, predicting and transactional monitoring techniques. For example, a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks; a new system that might be susceptible to fraud or abuse, and if so whether it ensures that the system has the capability for transactional level monitoring so you can audit the transactions if needed as part of an investigation.	N	
9.2	Automated decision making with legal or similar significant effect - processing that aims at taking decisions on individuals without human intervention. For example, the processing may lead to the exclusion or discrimination against individuals.	N	
9.3	Systematic monitoring of individuals* (e.g. CCTV, body camera's, health data through wearable devices) processing used to observe, monitor or control individuals. For example, monitoring of the	N	

<b>Q</b>	<b>Screening question</b>	<b>Y/N</b>	<b>Justification for response</b>
	employees' work station, internet activity, etc.		
<b>9.4</b>	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 subject	N	
<b>9.5</b>	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.).	N	
<b>9.6</b>	Innovative use or applying new technological or organisational solutions - combining the use of finger print and face recognition for improved physical access control. Implementation of a new technology, system or business process or collection of new information	N	
<b>9.7</b>	Offer online services directly to children	N	
<b>9.8</b>	Storing or transferring data outside the EU (e.g. cloud computing, accessing data outside the EU, use of an	N N	

Q	Screening question	Y/N	Justification for response
	American transcribe company)		
9.9	Direct marketing (e.g. newsletters, postcards, telemarketing, e-mail subscriptions)	N	
If you have answered "Yes" to any of the questions numbered 1-9 please proceed and complete stage 2.			
10	Is a <a href="#">Patient Safety</a> Review required?	N	
11	Is a Quality Impact/Technical Security Review required?	Y	Microsoft is ISO27001 compliant <a href="https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001">https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001</a>  <a href="https://docs.microsoft.com/en-gb/azure/compliance/">https://docs.microsoft.com/en-gb/azure/compliance/</a>

**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?	<input type="checkbox"/>	Revised/changed?	<input type="checkbox"/>	Other?	<input type="checkbox"/>
	If Other please specify.		No Change    X			



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


2.2.2	Is the data?					
	Identifiable?	<input type="checkbox"/>	Pseudonymised?	<input checked="" type="checkbox"/>	Anonymised?	<input type="checkbox"/>
	If the data is pseudonymised please describe 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. Also describe how the data will be transferred ie using HL7					
	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.					

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response <b>Yes or No</b>
	Y	To ensure data collection corresponds to the correct patient
2.3.1	How will you collect, use, store and delete data?	
	Collected with explicit written consent of the patient following a detailed discussion and information provided. Information collected via medical and electronic records.	
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, ICE and case notes	
2.3.3	How much data will you be collecting and using?	
	Patient initials, DOB, Research trial information specific to the trial assigned to Sealed envelope.	
2.3.4	How often? (for example monthly, weekly)	
	Data is collected and recorded ad-hoc on a daily basis, and after trail visits. Weekly, Monthly. Trial dependant.	
2.3.5	How long will you keep it?	
	<a href="https://www.sfh-tr.nhs.uk/media/12002/isp-101-records-management-code-of-practice-2021.pdf">https://www.sfh-tr.nhs.uk/media/12002/isp-101-records-management-code-of-practice-2021.pdf</a> Data collected must be retained for 20 years once the study has closed.	
2.3.6	Where will the data be stored? i.e. Medway, Shared Drive, offsite storage	
	Data obtained for the Sealed envelope system is stored in Medical notes, shared drive and clinical systems such as ICE, CareFlow EPR. All data is collected from source documents before entered into the database.	

2.3.7	How many individuals are affected?
	Unknown – Any research participant eligible for the trials that use this system.
2.3.8	What geographical area does it cover?
	Mansfield, Ashfield, Newark and Sherwood patients. Derbyshire patients ? Local / UK

2.4	Who are the Organisations involved in processing (sharing) the data?	
	Organisations Name	Data Controller or Data Processor  <i>The <b>Data Controller</b> 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.</i>  <i>The <b>Data Processor</b>, 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.</i>
	Sealed envelope and Sherwood Forest Hospitals NHS Foundation Trust	Data Controller and processor  Processor – the Trust control their own data but also processes data for the overall data to the sponsor through sealed envelope.
	Microsoft Azure	Sub data processor

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	
	<b>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</b>	
	 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 <a href="https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001">https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001</a>		
2.5.1	Please describe access and controls in place  <a href="https://www.sfh-tr.nhs.uk/media/12007/ig-012-account-management-and-access-policy-2021.pdf">https://www.sfh-tr.nhs.uk/media/12007/ig-012-account-management-and-access-policy-2021.pdf</a>   Account ManagementSOP Terr		
	User account management is the responsibility of the Sponsor manager of the trial using Sealed envelope for data capture. The Trust does not manage access, it is the trial team. The Trust to ensure that the supplier is informed of movers and leavers.		
2.5.2	Please provide a copy of the contract in place		
	There is no formal contract in place.		
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 <a href="#">register</a>	Yes	No
		X	
2.5.5	Has the supplier received ICO Enforcement? Please check the <a href="#">register</a>	Yes	No
			X
2.5.6	Has the supplier received ICO Decision Notice? Please check the <a href="#">register</a>	Yes	No
		x10 in relation to Freedom of Information Act	
2.5.7	Has the supplier received an ICO Audit? Please check the <a href="#">register</a>	Yes	No
			x

<b>2.5.8</b>	Has the supplier completed a Data Security and Protection Toolkit, please check the <a href="#">register</a> and provide the following details	Completed: Yes/No	Date submitted	Standard Met/Not Met
		Yes	10 <sup>th</sup> October 2022	Standards Met
<b>2.5.9</b>	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 <a href="https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001">https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001</a>		
	ISO 9001 Quality Management Systems	Microsoft <a href="https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-iso-9001?toc=/compliance/regulatory/toc.json&amp;bc=/compliance/regulatory/breadcrumb/toc.json">https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-iso-9001?toc=/compliance/regulatory/toc.json&amp;bc=/compliance/regulatory/breadcrumb/toc.json</a>		
<b>2.5.10</b>	Is the data held outside of the UK ie Europe, USA, Ireland? If yes please include the country			
	Yes	No		
		X		
	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 <b>Yes</b> please describe organisation/s and geographic location			
	N				
2.7	Does the work involve employing contractors external to the Organisation?				
	Y/N	If <b>Yes</b> , provide a copy of the confidentiality agreement or contract?			
	N				
2.8	Has a data flow mapping exercise been undertaken?				
	Y/N	If <b>Yes</b> , 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 <b>No</b> , please complete – Section 3			
	N	The Trust will need to map the flow of data for this service. Added as a risk to the DPIA.			
2.9	What format is the data?				
	Electronic	<input checked="" type="checkbox"/>	Paper	<input type="checkbox"/>	Other (Please describe)
2.10	Is there an ability to audit access to the information?				
	Y/N	Please describe if answered <b>Yes</b> . If <b>NO</b> what contingencies are in place to prevent misuse?			
	Y	<p>Audit log on database. The audit log captures the following items</p> <ul style="list-style-type: none"> <li>· Time and Date of action</li> <li>· User performing the action</li> <li>· The type of action and context performed</li> <li>· Data change / action</li> </ul> <p>The type of action which the audit log will capture are: Create / Delete / Insert / Merge / Update / Reorder.</p> <p>Any End-User who has been provided with Administrative permissions can access and query the audit log.</p>			

<b>2.11</b>	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 <b>Yes</b>
	N	
<b>2.12</b>	How will the information be kept up to date and checked for accuracy and completeness? (data quality) How will you ensure data minimisation?	
	Monitor reports 3 monthly. The right to rectification - People can inform us if they think we hold inaccurate information about them. These requests will be considered on a case-by-case basis.	
<b>2.13</b>	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 sponsor.	
<b>2.14</b>	What security measures have been implemented to secure access?	
	Active Directory (Window's username and password)	<input type="checkbox"/>
	Username and password	<input checked="" type="checkbox"/>
	Smartcard	<input type="checkbox"/>
	Key locked filing cabinet/room	<input type="checkbox"/>
	Hard/soft Token (VPN) Access	<input type="checkbox"/>
	Restricted Access to Network Files (shared drive)	<input type="checkbox"/>
	Has information been anonymised?	<input type="checkbox"/>
	Has information been pseudonymised?	<input checked="" type="checkbox"/>
	Is information fully identifiable?	<input type="checkbox"/>
Other (provide detail below)	<input type="checkbox"/>	

<b>2.15</b>	Will the data be stored on Trust servers			
	Yes	No		
		x		
<b>2.16</b>	Please state by which method the information will be transferred?			
	Email (not NHS.net)	<input type="checkbox"/>	NHS.net	<input type="checkbox"/>
	Website Access (internet or intranet)	<input checked="" type="checkbox"/>	Wireless Network (Wi-Fi)	<input type="checkbox"/>
	Secure Courier	<input type="checkbox"/>	Staff delivered by hand	<input type="checkbox"/>
	Post (internal)	<input type="checkbox"/>	Post (external)	<input type="checkbox"/>
	Telephone	<input type="checkbox"/>	SMS	<input type="checkbox"/>
	Fax	<input type="checkbox"/>	Other (please specify below)	<input type="checkbox"/>
	<p>N/A – No identifiable data is transferred. Data will be uploaded via secure portal. SSL (Security Socket Layer) and HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) are used in the encrypted transmission of data. In order to ensure that data are accessed as expected, we have taken the following measures:</p> <ol style="list-style-type: none"> <li>1. A firewall is used to filter malicious access.</li> <li>2. Intrusion detection is used to detect system anomalies.</li> <li>3. Malicious Code Protection is used to perform security checks on all committed data.</li> </ol>			
<b>2.17</b>	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 <b>Yes</b> . Please state why not if response is <b>No</b> .										
	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.										
<b>2.18</b>	Has staff training been proposed or undertaken and did this include confidentiality and security topics areas?											
	Y/N	Please describe if answered <b>Yes</b>										
	Y	All those given access to database are required to receive training by the Sponsor leading the trial using sealed envelope.										
<b>2.19</b>	Will reports be produced?											
	Will reports contain personal/sensitive personal or business confidential information?	N										
	Who will be able to run reports?	Sponsor										
	Who will receive the reports and will they be published?	Those delegated to the trial and with permission										
<b>2.20</b>	If this new/revised function should stop, are there plans in place for how the information will be <b>retained / archived/ transferred or disposed of</b> ?											
	Y/N	Please describe if answered <b>Yes</b> . Please state why not if response is <b>No</b> .										
	Y	A copy of the trial consent and participant information sheet (PIS) Case report forms as well as nursing notes will be in the patient's medical records, along with being retained in the study site file.										
	<table border="1"> <thead> <tr> <th colspan="2">TERMINATION &amp; EXIT</th> </tr> </thead> <tbody> <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: <ul style="list-style-type: none"> <li>- Exit Management Transition Schedule</li> <li>- Exit Management Data Extraction Format and Requirements</li> </ul> </td> </tr> <tr> <td>Will the supplier remove all subscriber data from 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> </tbody> </table>		TERMINATION & EXIT		Upon contract termination notice will an exit manager be designated by the supplier for the notice period?	Yes – The subscriber account manager will also provide exit manager services upon contract termination notice	What exit management requirements will be required from subscriber?	Subscriber will need to provide supplier with: <ul style="list-style-type: none"> <li>- Exit Management Transition Schedule</li> <li>- Exit Management Data Extraction Format and Requirements</li> </ul>	Will the supplier remove all subscriber data from the database and back-ups upon termination of service?	Yes	Will the supplier issue a Data Destruction Certificate to confirm removal of all subscriber data?	Yes – Upon contract termination the data destruction process will be initiated
TERMINATION & EXIT												
Upon contract termination notice will an exit manager be designated by the supplier for the notice period?	Yes – The subscriber account manager will also provide exit manager services upon contract termination notice											
What exit management requirements will be required from subscriber?	Subscriber will need to provide supplier with: <ul style="list-style-type: none"> <li>- Exit Management Transition Schedule</li> <li>- Exit Management Data Extraction Format and Requirements</li> </ul>											
Will the supplier remove all subscriber data from the database and back-ups upon termination of service?	Yes											
Will the supplier issue a Data Destruction Certificate to confirm removal of all subscriber data?	Yes – Upon contract termination the data destruction process will be initiated											

2.21	Is consent required for processing of personal data?	
	Y/N	Please describe if answered <b>Yes</b>
	Y	Consent to the study given
		If <b>No</b> , 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?
2.22	Will individuals be informed about the proposed uses and share of their personal data?	
	Y/N	Please describe if answered <b>Yes</b> . Please state why not if response is <b>No</b> .
	Y	How data is used is explained in the study participant information sheet and consent form. The Trust's privacy notice is here <a href="https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/">https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/</a> . The research team have reviewed the patient privacy notice and no more detail is required.
2.23	Is there a process in place to remove personal data if data subject refuses/removes consent	
	Y/N	Please describe if answered <b>Yes</b> . Please state why not if response is <b>No</b> .
	Y	Personal data for patients who dissent is not captured. When a patient of a research study removes consent their existing data will remain but no further data is collected.
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 <b>Yes</b> . Please state why not if response is <b>No</b> .
	Y	How data is used is explained in the study participant information sheet in addition to the consent form

2.25	Are arrangements in place for recognising and responding to requests for access to personal data?	
	Y/N	Please describe if answered <b>Yes</b> . Please state why not if response is <b>No</b> .
	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: <a href="http://Sherwood Forest Hospitals (sfh-tr.nhs.uk)">Sherwood Forest Hospitals (sfh-tr.nhs.uk)</a>
2.26	Who are the Information Asset Owner(s) and Administrator(s)?	
	IAO	Alison Steel
	IAA	Terri-Ann Sewell/Rachel Boddice
	System Administrators	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 <b>Yes</b> . Please state what checks were undertaken if response is answered <b>No</b> .
	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.
2.29	Are there any current issues of public concern that you should factor in?	
	Y/N	Please describe if answered <b>Yes</b> .
	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?	

	Sealed Envelope is used to maintain an overview of the Research data collected for a patients trial journey to help answer the research question. It allows us to access opportunities for wider patient involvement in Research and improve treatment and care.
<b>2.31</b>	<p>Consider how to consult with relevant stakeholders:</p> <ul style="list-style-type: none"> <li>• Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so.</li> <li>• Who else do you need to involve within your organisation?</li> <li>• Do you need to ask your processors to assist?</li> </ul> <p>Alison Steele presented this document to the Information Governance working group for consultation.</p>

<b>2.32</b>	<p>What is your lawful basis for processing? (please see <a href="#">Appendix 10</a> Information Sharing Protocol for further information). <b>Consent is usually the last basis to rely on</b></p> <p><b>Legal basis: patients</b></p> <p><b>Personal data i.e. name, address</b></p> <p>6(1)(a) the patient has given consent</p> <p>6(1)(c) necessary for legal obligations</p> <p>6(1)(e) public interest or public duty</p> <p>6(3) the above supported by Member State law (UK legislation as applicable to circumstances)</p> <p><b>Sensitive personal data (special category)</b></p> <p>9(2)(a) the patient has given explicit consent</p> <p>9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc.)</p> <p>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).</p> <p>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.</p>
-------------	--

	<p>9(2)(j) (together with Article 89 and relevant recitals) relates to archiving, statistical analysis and research.</p> <p><b>Legal basis: staff</b> – please review <a href="#">Appendix 10</a> Information Sharing Protocol for further information).</p>
	<p>6(1)(a) the patient has given consent</p> <p>9(2)(a) the patient has given explicit consent</p>
<b>2.33</b>	<p>What information will you give individuals about the processing? (This information will be added to the Trust’s Patient <a href="#">Privacy Notice</a> and Staff <a href="#">Privacy Notice</a> by the Information Governance Team)</p>
	<p>Study Participant Information Sheet, Consent Form, Verbal Instruction. This DPIA will be published once finalised. The Trust’s privacy notice does not need to be updated.</p>
<b>2.34</b>	<p>What measures do you take to ensure processors comply?</p>
	<p>Identifiable data retained and processed by the Trust Research &amp; Innovation staff only.</p>
<b>2.35</b>	<p>How will you prevent function creep? Manage lifecycle of system/process</p>
	<p>Controlled by development team at University of Southampton</p>



## Stage - 3 Risk Template

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

Completed by: Donna Sowter  
Gina Robinson, Information Security Officer updated 15<sup>th</sup> June 2022

Role: Research Support Facilitator / Information Manager

Date completed: 21<sup>st</sup> April 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)	
<p>Loss of system access due to connection failure or server failure either via NHIS or 3<sup>rd</sup> party supplier.</p> <p>This could result in the service being disrupted or unavailable.</p> <p>The consequences of this could be enforcement action and reputational damage to the Trust</p>	<p>Full system back-up processes and ISO 27001 accreditation in place</p> <p>Business continuity plan in place</p> <p>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</p>	2	2	4		2	2	4	
<p>Loss of system data due to system failure and/or backup failure either via NHIS or 3<sup>rd</sup> party supplier.</p> <p>This could result in the service being disrupted or unavailable.</p> <p>The consequences of this could be enforcement action and reputational damage to the Trust</p>	<p>Full system back-up processes and ISO 27001 accreditation in place.</p> <p>Business continuity plan in place</p> <p>All data entered onto the database is also available in paper form and where electronic it is saved to the shared drive.</p>	2	2	4		2	2	4	

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 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. Access is managed by the supplier. The research team will provide the supplier with a list of movers and leavers as appropriate. Appropriate access according to role. IG Training in place.	3	1	3		3	1	3	



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
<p><b>Principle 1 –</b> Personal data shall be processed fairly and lawfully and, in a transparent manner</p>	<p>Lawfulness</p> <ul style="list-style-type: none"> <li>• We have identified an appropriate lawful basis (or bases) for our processing.</li> <li>• We are processing special category data and have identified a condition for processing this type of data.</li> <li>• We don't do anything generally unlawful with personal data.</li> </ul> <p>Fairness</p> <ul style="list-style-type: none"> <li>• We have considered how the processing may affect the individuals concerned and can justify any adverse impact.</li> <li>• We only handle people's data in ways they would reasonably expect, or we can explain why any unexpected processing is justified.</li> <li>• We do not deceive or mislead people when we collect their personal data.</li> </ul> <p>Transparency</p> <ul style="list-style-type: none"> <li>• We are open and honest, and comply with the transparency obligations of the right to be informed.</li> </ul>
<p><b>Principle 2 –</b> Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes</p>	<ul style="list-style-type: none"> <li>• We have clearly identified our purpose or purposes for processing.</li> <li>• We have documented those purposes.</li> <li>• We include details of our purposes in our privacy information for individuals.</li> <li>• We regularly review our processing and, where necessary, update our documentation and our privacy information for individuals.</li> <li>• 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</li> </ul>

	our original purpose or we get specific consent for the new purpose.
<b>Principle 3 –</b> Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	<ul style="list-style-type: none"> <li>• We only collect personal data we actually need for our specified purposes.</li> <li>• We have sufficient personal data to properly fulfil those purposes.</li> </ul>
<b>Principle 4 –</b> 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	<ul style="list-style-type: none"> <li>• We ensure the accuracy of any personal data we create.</li> <li>• We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data.</li> <li>• 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.</li> <li>• If we need to keep a record of a mistake, we clearly identify it as a mistake.</li> <li>• Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts.</li> <li>• We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data.</li> <li>• As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data</li> </ul>
<b>Principle 5 –</b> Kept no longer than is necessary	<ul style="list-style-type: none"> <li>• We know what personal data we hold and why we need it.</li> <li>• We carefully consider and can justify how long we keep personal data.</li> <li>• 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.</li> </ul>
<b>Principle 6 –</b> Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage	<ul style="list-style-type: none"> <li>• 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.</li> </ul>

	<ul style="list-style-type: none"><li>• 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.</li><li>• We use encryption.</li><li>• We understand the requirements of confidentiality, integrity and availability for the personal data we process.</li><li>• 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.</li><li>• 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.</li><li>• We implement measures that adhere to an approved code of conduct or certification mechanism.</li><li>• We ensure that any data processor we use also implements appropriate technical and organisational measures.</li></ul>
--	---