

# Data Protection Impact Assessment

Title	Ref number
<b>Fairwarning SAS Migration (Imprivata)</b>	

## Introduction

A Data Protection Impact Assessment enables Sherwood Forest Hospitals NHS Foundation Trust (SFHFT) 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	x	x
Complete Project Details and check the Initial Screening Questions	x	x

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	X	X
Initial Screening Questions to be formally written up and Introductory Meeting to be formally recorded	X	X

**If a Data Protection Impact Assessment IS NOT required**

<b>Activity</b>	<b>IAO</b>	<b>Governance</b>
Complete Assessment Summary & Recommendations for Action	X	X
Assessment to be passed to Implementer		X
Ensure Sign Off is completed	X	X
Assessment shared with customer if appropriate	X	
Assessment to be kept with project documentation copy to Information Governance	X	

**OR**

**If a Data Protection Impact Assessment IS required**

<b>Activity</b>	<b>IAO/IAA</b>	<b>Governance</b>
When a new system is being implemented and the supplier provides a completed DPIA on a suppliers template, the information will need to be transferred to the Trust’s template to ensure there are no omissions	X	
Complete Stage 2 – Data Protection Impact Assessment (Full)	X	
Complete Stage - 3 Identified Risks and Mitigating Action	X	
Complete Stage – 4 Legal Compliance		X
Complete Assessment Summary & Recommendations for Action	X	
Account access management Standard Operating Procedure to be completed prior to the implementation of the project	X	
Closure meeting for final agreement	X	
Ensure Sign Off is completed		X
Assessment shared with customer if appropriate	X	
Assessment to be kept with project documentation copy to Information Governance	X	

**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>Fairwarning SAS Migration</b>
-----------------------	----------------------------------

### **Project Description: Describe in sufficient detail for the proposal to be understood**

FairWarning is a software solution which was purchased in 2015 to support the Information Governance requirements to conduct 'active' monitoring of users access to electronic systems containing sensitive personal information. FairWarning uses a number of parameters to identify potential inappropriate access, for example, access to patient records of an individual who is not currently receiving treatment e.g. deceased patient records, and/or access to a patient record of a user with the same surname.

The current version of Fairwarning is has now become outdated/out of warranty hardware which poses the risk of failure and could lead to loss of data. The proposal is to move to a SAAS (cloud environment). This would mean the Trust is on the most up to date version all the time which would eliminate all immediate and future costs of hardware (internal and external).

With the move to a more digital records environment for the Trust this poses a greater risk for inappropriate access to records. Therefore the update will also include the move to adding the Nervecentre feed and ESR feed, which will enrich the current results.

### **Overview of the proposal: What the project aims to achieve**

.Implementation of the product includes the below benefits

- Reduced risk of fines from the ICO
- Reduced number of information breaches
- Improved corporate reputation
- Improved compliance with the CQC, IG Toolkit and Care Record Guarantee
- Enhance application performance for end-users and support future releases of AI and Machine Learning advancements – always on the most up to date version
- Immediate storage solution (4TB) and flexible options for on-demand scal
- Improved application services support and automated data deliveries

- Eliminate single end-point/point of failure
- Multiple backups for increased disaster recovery – managed by Imprivata FairWarning
- More predictability & efficiency for all resources (time, upgrades, budgets)

The need to review the previous DPIA arises as we move to a new product environment and security changes.

- the need for constant monitoring of staff who access records within the Orion system and the production of reports based on the audit trails and the parameters set out above
- more staff having routine access to audit information rather than on an ad-hoc basis in response to a reported incident
- the good practice of assessing all projects via DPIA

Remaining on the old version of Fairwarning means that being out of compliance can cost significantly more to recover data and repair the hardware than the total of the SaaS conversion.

<b>Implementing Organisation:</b>	Sherwood Forest Hospitals NHS Foundation Trust
-----------------------------------	--

<b>Staff involved in DPIA assessment (name and job title):</b>	Jacque Widdowson, IG Manager/DPO
--	----------------------------------

### Project Sign Off

	Name	Job Title	Organisation	Date
<b>Information Asset Owner</b>	Jacque Widdowson	IG Manager/DPO	Sherwood Forest Hospitals NHS Foundation Trust	
<b>Data Protection Officer</b>	Jacque Widdowson	Information Governance Manager/DPO	Sherwood Forest Hospitals	

			NHS Foundation Trust	
<b>Information Governance</b>	Jacque Widdowson	Information Governance Manager/DPO	Sherwood Forest Hospitals NHS Foundation Trust	1/06/2023
<b>Senior Information Risk Owner</b>	Sally Brook-Shanahan	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	
<b>Caldicott Guardian</b>	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	
<b>Chief Digital Information Officer</b>	Richard Walker	Chief Digital Information Officer	Sherwood Forest Hospitals NHS Foundation Trust	

## 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 checked="" type="checkbox"/>
3. Project/Implementation has met required legislative compliance and poses not significant risks. No further action required.	<input type="checkbox"/>

**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/data - Full system back-up process in place
2. Leavers' access not removed - xx system team notified of leavers by HR. Changes to user roles reviewed monthly via a Trust e-form report
3. Business continuity plans in each area, users have business continuity plans for their areas/departments. Not having these could lead to access to data problems or service delivery problems.
4. Fairwarning will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO
5. 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.

## Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	Recommendation Owner:	Agreed Deadline for action:
Account management Standard Operating Procedure generated and implemented, routine audit to take place	IAA	TBC – once project has been agreed
Commence staff awareness campaign	IAA	Already implemented, quarterly staff Bulletin
Staff to undertake annual IG Training	IAA	All staff annually
Staff who will use the system to undertake Fairwarning training	IAA	TBC – once project has been agreed



## 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 processing of information about individuals	Y	<b>Principle 6 –</b> Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage
2	Will the project compel individuals to provide information about themselves?	N	<b>Principle 6 –</b> Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	N	<b>Principle 6 –</b> Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage
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	<b>Principle 6 –</b> Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	The information within Active Directory needs to be accurate and up to date in order for reports to be correct and meaningful.

Q	Screening question	Y/N	Justification for response
6	Are there security arrangements in place while the information is held?	Y	
7	Does the project involve using new technology being introduced?	Y	Fairwarning is already in place within the organisation. This is moving the system to a SaaS environment
8	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	Y	Potentially disciplinary for staff member who accesses information inappropriately.
9	Does the project include any of the following activities? (Mark all that apply and a description if answered 'Y')		
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	N/A
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	N/A
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 employees' work station, internet activity, etc.	Y	Monitoring staff who have inapprpriately accessed a patients medical records. <b>Principle 6 –</b> Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage

Q	Screening question	Y/N	Justification for response
9.4	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	N/A
9.5	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>Principle 6 –</b> Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage
9.6	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>Principle 6 –</b> Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage  Information is already collected, just moving to a new environment
9.7	Offer online services directly to children	N	N/A
9.8	Storing or transferring data outside the EU (e.g. cloud computing, accessing data outside the EU, use of an American transcribe company)	N	N/A
9.9	Direct marketing (e.g. newsletters, postcards, telemarketing, e-mail subscriptions)	N	N/A
<b>If you have answered “Yes” to any of the questions numbered 1-9 please proceed and complete stage 2.</b>			
10	Is a Patient Safety Review required? <a href="#">DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital</a>	N	N/A

Q	Screening question	Y/N	Justification for response
11	Is a Quality Impact/Technical Security Review required?	Y	

**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 checked="" type="checkbox"/>	Other?	<input type="checkbox"/>
	If Other please specify.					





2.2.1	What data will be processed?					
	<b>Personal Data:</b>					
	Forename	<input checked="" type="checkbox"/>	Surname	<input checked="" type="checkbox"/>	Age	<input type="checkbox"/>
	DOB	<input checked="" type="checkbox"/>	Gender	<input type="checkbox"/>	Address	<input checked="" type="checkbox"/>
	Post Code	<input checked="" type="checkbox"/>	NHS No	<input checked="" type="checkbox"/>	Hospital No	<input checked="" type="checkbox"/>
	Other unique identifier (please specify)					
	<b>Sensitive Personal Data (special categories):</b>					
	Children					<input checked="" type="checkbox"/>
	Vulnerable groups					<input checked="" 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					<input type="checkbox"/>
	Sexual Health					<input type="checkbox"/>
	Criminal offence data					<input type="checkbox"/>
	Other data (please specify)					

<b>2.2.2</b>	Is the data?					
	Identifiable?	<input checked="" type="checkbox"/>	Pseudonymised?	<input 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.					
<b>2.3</b>	Is the data required to perform the specified task?					
	Y/N	Please justify response <b>Yes or No</b>				
	Y	<p>Yes to prevent inappropriate access to medical records and investigate all instances of inappropriate access.</p> <p><b>Principle 6 –</b> Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage</p>				
<b>2.3.1</b>	How will you collect, use, store and delete data?					
	<p>The data will be collected by Fairwarnig from Trust systems</p> <p>Data will be stored in a cloud environment</p> <p>Data will be deleted in line with Records Management Code of Practice</p>					
<b>2.3.2</b>	What is the source of the data? (i.e. from data subject, system or other third party)					
	The source of the data will be from the system.					
<b>2.3.3</b>	How much data will you be collecting and using?					
	Using ESR, ORION and Nervencentre data in the first instance					
<b>2.3.4</b>	How often? (for example, monthly, weekly)					
	Daily report received from Fairwarning to indicate who has inappropriately accessed records.					

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>
	In line with the records management code of practice
2.3.6	Where will the data be stored? i.e., CareFlow, Shared Drive, offsite storage AWS Secure Data Centre
2.3.7	How many individuals are affected?
	The number of affected individuals is around 4,500, could be more
2.3.8	What geographical area does it cover?
	Mansfield, Ashfield, Newark and Sherwood patients. Derbyshire patients

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>
	Sherwood Forest Hospitals NHS Foundation Trust	Data Controller
	Imprivita	Data Processor

2.5	If we have identified a supplier in 2.4, the following questions for 2.5 will need to be answered by the <b>supplier and the Trust</b>	
	Y/N	<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>

		 Supplier Assurance Framework TEMPLATI  Supplier Assurance Framework - Example  Cloud Assessment.xlsx				
		NHIS have reviewed the attachments and assessed as low risk.				
2.5.1	<p>Please describe access and controls in place</p> <p>Account access management Standard Operating Procedure to be completed prior to the implementation of the project</p> <p><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></p>  Account Management & Acces					
	<p>Fairwarning retain a secure record of the data in the Cloud and the data is only accessible to the individual and the organisations/individuals the patient wishes to share with. In order to ensure the confidentiality of patients' data, Fairwarnign have taken the following measures:</p> <ol style="list-style-type: none"> <li>1. Fairwarnign is accessed by using AD credentials .</li> <li>2. Different types of users have different access levels.</li> </ol>					
2.5.2	<p>Please provide a copy of the contract in place</p> <p>Available on request</p>					
2.5.3	<p>Have arrangements for retention and destruction been included in the contract when the service/contract expires?</p> <p>To be returned to SFH</p>					
2.5.4	<p>Is the supplier registered with the ICO? Please check the <a href="#">register</a></p>	<table border="1"> <tr> <td>Yes</td> <td>No</td> </tr> <tr> <td>Y</td> <td></td> </tr> </table>	Yes	No	Y	
Yes	No					
Y						
2.5.5		<table border="1"> <tr> <td>Yes</td> <td>No</td> </tr> </table>	Yes	No		
Yes	No					



	Has the supplier received ICO Enforcement? Please check the <a href="#">register</a>			<b>N</b>
<b>2.5.6</b>	Has the supplier received ICO Decision Notice? Please check the <a href="#">register</a>		Yes	No
				N
<b>2.5.7</b>	Has the supplier received an ICO Audit? Please check the <a href="#">register</a>		Yes	No
				N
<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
		Y		
<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	Y		
	ISO 15489 Records Management		N	
	ISO 27001 Information Security Standards	Y		
	ISO 9001 Quality Management Systems		N	
<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		
		N		
	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. If No, please explain why			
	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 explain why				
	Y the system has been added to the IG data flow map and IAR				
2.9	What format is the data?				
	Electronic	<input checked="" type="checkbox"/>	Paper	<input type="checkbox"/>	Other (Please describe) <a href="#">Click here to enter text.</a>
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	Audit trails are available to see who has accessed the information			
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 <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?	
	<p>Staff new starters and leavers will be added/disabled as and when. Any discrepancies are investigated. Staff are encouraged to update there address details on ESR.</p> <p>Data quality exercises are undertaken by the Trust to ensure accurate data from patients.</p> <p>Only data that is required to perform the task is needed and no excessive data is collated.</p>	
<b>2.13</b>	Who will have access to the information? (list individuals or staff groups)	
	<p>Members of the Information Governance Team will have access to the Fairwarning product.</p> <p>Any members of staff who have inappropriately accessed information, will have their details forwarded to the relevant line manager and HR.</p>	
<b>2.14.1</b>	What security measures have been implemented to secure access?	
	Active Directory (Window's username and password)	<input checked="" type="checkbox"/>
	Username and password	<input 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 type="checkbox"/>
	Is information fully identifiable?	<input checked="" type="checkbox"/>

	Other (provide detail below)		<input type="checkbox"/>
<b>2.14.2</b>	What physical security measures have been implemented to secure access? ie swipe cards, digilock		
	Physical access to the server rooms and remote access to the servers is restricted to those who require access to perform their duties.		
<b>2.15</b>	Will the data be stored on Trust servers		
	Yes	No	
		N	
<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"/>
	Other	<input type="checkbox"/>	please specify below <input type="checkbox"/>
	<p>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>		

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 <b>Yes</b> . Please state why not if response is <b>No</b> .
	Y	Once the system is back up and running business will commence as usual with time and resource allocated to any backlog created. The system is not an essential clinical service.
2.18	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>
		All employees at the Trust have received IG Mandatory Training, which includes elements of the DPA 2018  Trust employees will receive training on how to use the Fairwarning system.
2.19	Will reports be produced?	
	Will reports contain personal/sensitive personal or business confidential information?	Y
	Who will be able to run reports?	Members of the IG Team
	Who will receive the reports and will they be published?	IG Team will receive the reports and will publish figures to the IG Committee and associated meetings. No PID will be shared within the reports.
2.20	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	Return to SFH
2.21	Is consent required for processing of personal data?	
	Y/N	Please describe if answered <b>Yes</b>
	N	
		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?
	N	UK GDPR 6(1)(c) processing is necessary for compliance with a legal obligation to which the controller is subject UK GDPR 6(1)(e) public interest or public duty  To prevent breach of principle 6 of the DPA
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	The right to be informed - Transparency information and materials on the virtual ward will be available to people when they are admitted to the ward. This information will also be available on all participating organisations' websites. 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 right to object - People can object to their information being used for any purpose, and these objections will be considered on a case-by-case basis.
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> .
	N	<p>The right to restrict processing - People can request the use of their data to be restricted in certain circumstances. These will be considered on a case-by-case basis.</p> <p>The right to data portability - Not applicable in this circumstance as the legal bases for processing the data are neither consent nor for the performance of a contract.</p> <p>The right to object - People can object to their information being used for any purpose, and these objections will be considered on a case-by-case basis.</p>
<b>2.24</b>	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	Patients and staff would expect staff to monitor their privacy and any inappropriate access identified acted upon.
<b>2.25</b>	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> .
	Y	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://www.sherwoodforesthospitals.nhs.uk">Sherwood Forest Hospitals (sfh-tr.nhs.uk)</a>
<b>2.26</b>	Who are the Information Asset Owner(s) and Administrator(s)?	
	IAO	IG Manager/ DPO
	IAA	IG Team

	System Administrators	IG Team
2.27	How is the data secured in transit and at rest? Eg encryption, port control number	
	<p>The data is transmitted via HL7 and encrypted both in transit and at rest. HL7 - Health Level Seven® International (HL7®) is the global authority on standards for interoperability of health technology and is the global industry standard for passing healthcare data between systems.</p> <p>Or</p> <p>In order to maintain data integrity and security, we use SSL (Secure Socket Layer) server certificate to secure its diabetes management portal: to provide encryption for the data being transferred between the server, the patient and clinician. This helps to prevent eavesdropping attacks on the data and third-party accessing to the data.</p>	
2.28	Has the impact to other NHIS systems/processes been considered and appropriate SBU's consulted and in particular technical security?	
	Y/N	<p>Please describe if answered <b>Yes</b>. Please state what checks were undertaken if response is answered <b>No</b>.</p> <p><a href="#">DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital</a></p>
		A patient safety case and supplier assurance framework have both been reviewed by NHIS. No risks or recommendations identified.
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	Non identified
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?	
	<p>Implementation will mean:</p> <ul style="list-style-type: none"> <li>• Reduced risk of fines from the ICO</li> <li>• Reduced number of information breaches</li> </ul>	



	<ul style="list-style-type: none"> <li>• Improved corporate reputation</li> <li>• Improved compliance with the CQC, DSP Toolkit and Care Record Guarantee</li> <li>• Assurance that adhering to principle 6 of the DPA is appropriate, Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage</li> </ul>
<p><b>2.31</b></p>	<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>IG Manager/ DPO presented this document to the Information Governance working group for consultation.</p> <p>Sign off will be obtained from SIRO, Caldicott and CDIO</p>

<p><b>2.32</b></p>	<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>The Trust’s lawful basis for processing personal and special categories of personal data are:</p> <ol style="list-style-type: none"> <li>1. UK GDPR 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.</li> <li>2. UK GDPR 9(2)(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject</li> <li>3. 6(1)(c) necessary for legal obligations</li> </ol> <p>Supplier</p> <ol style="list-style-type: none"> <li>1. UK GDPR 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.</li> </ol>
<p><b>2.33</b></p>	<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>This DPIA will be published once finalised. The Trust’s privacy notice has been updated. .</p>

	<p>Communication campaign for staff to inform the system is in place and will be monitoring in appropriate access. This will be communicated several times a year for the life time of the project.</p>
<b>2.34</b>	<p><b>What measures do you take to ensure processors comply?</b></p> <p>The Trust is not aware of any sub processors involved in this project, for which it is responsible for ensuring compliance</p> <p>The Trust and Fairwarning have a contract in place and this will be reviewed on a regular basis.</p> <p>Relevant certifications will be requested on an annual basis to review compliance.</p>
<b>2.35</b>	<p><b>How will you prevent function creep? Manage lifecycle of system/process</b></p> <p>Fairwarning will only ever process the Trust's data as per explicit agreement with the Trust</p> <p>From a lifecycle management point of view a report to SIRO will be undertaken annually, this will provide an update on the phases of implementation, operationally and termination</p> <p>Any new iterations of the system will be included in the report to SIRO and the DPIA will be reviewed.</p>

## Stage - 3 Risk Template

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

Completed by:	Role:	Date completed:
---------------	-------	-----------------

<b>Risk description</b> What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	<b>Primary controls</b> What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	<b>Current risk</b>			<b>Gaps in control</b> If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	<b>Acceptable risk</b>			<b>Mitigating actions required</b> 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)	
<b>Privacy &amp; Security Risk</b>  Loss of system  This could result in the service being disrupted or unavailable.  The consequences of this could be financial penalties and reputational damage to the Trust	Full system back-up processes Manual input, business continuity plan to be used	2	2	4	No gaps in control identified	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)	
<b>Privacy &amp; Security Risk</b> 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.  Which could lead to loss or access to data  <b>Risk to individuals</b>  No monitoring of inappropriate access.. unable to identify breach	The system is not a clinical application therefore, downtime for several weeks could be tolerated.  Audits to be undertaken manually	2	2	4	Business continuity plan needs to be in put in place.	2	1	2	Develop a Business continuity plan reviewed annually.
<b>Privacy &amp; Security Risk</b>  Data is lost during the migration from old system to new system	Following migration of data the IG team will conduct a review of a selection of records to ensure the integrity of data transferred	3	2	6	Work would need to be undertaken with supplier to establish why the data did not migrate accurately and what actions can be taken to rectify	3	1	3	IG team to review records transferred to confirm integrity

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>Integrity of data is compromised</p> <p>Which could lead to loss of data</p> <p><b>Risk to individuals</b></p> <p>Not able to identify inappropriate access. Reputational damage and accusing wrong individual.</p>									
<p><b>Privacy &amp; Security Risk</b></p> <p>Constant monitoring of staff who access records within the Orion/ Nervecentre system and the production of reports based on the audit trails and the parameters set out above</p>	<p>Current Fairwarning solution in place</p> <p>Staff are currently notified that the use of Fairwarning is in place</p> <p>Staff attend IG training on an annual basis</p> <p>Part of terms and conditions of employment</p>	2	2	4	No gaps in control currently identified	2	1	2	<p>Awareness campaign notifying staff of its use to be reviewed and disseminated. This will include reminder of staff responsibilities in relation to maintaining confidentiality</p>

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)	
<b>Risk to individuals</b>  User information will be made available on a proactive basis rather than reactive. Staff may not be aware of their responsibilities in relation to accessing sensitive personal information and therefore may breach confidentiality	Contained in Trust Privacy Notice				No gaps identified				Privacy notice to be reviewed and ensure this references the use of Fairwarning.
<b>Privacy &amp; Security Risk</b>  More staff having routine access to audit information rather than on an ad-hoc basis in	Delegated staff who currently use the system are trained and understand the reports.	1	1	2	No gaps identified	1	1	2	All delegated staff will be trained on how to use the system and understand the reports produced

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>response to a reported incident</p> <p><b>Risk to individuals</b></p> <p>Delegated staff who have access to the reports need to recognise a bona fide breach from a legitimate reason for clinical access as a misunderstanding may lead to disciplinary action being taken unnecessarily</p>	<p>Training in place for those who are delegated to use the system.</p> <p>Support for training from Fairwarning and ongoing user queries.</p> <p>Robust investigation process in place.</p> <p>FairWarning provide client support for the lifetime of the system.</p>				No gap identified				Robust processes will need to be in place to ensure that reports have been verified prior to a detailed investigation being authorised
<p><b>Privacy &amp; Security Risk</b></p> <p>The information within Active Directory needs to be accurate and up to date in order for</p>	<p>Staff starters process in place.</p> <p>Process for leavers from the organisation in place</p> <p>Delegated staff trained on the use of the system</p>	2	2	4	<p>Damage to corporate reputation and possible financial penalty awarded</p> <p>Damage and distress on wrongly accused staff member.</p>	2	1	2	All delegated staff will be trained on how to use the system and understand the reports produced; including the



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>reports to be correct and meaningful</p> <p><b>Risk to Individual</b></p> <p>Staff may be wrongly accused of inappropriate access to records if their information is not kept up to date in Active Directory</p>								<p>identification of false-positive flags</p> <p>Robust processes will need to be in place to ensure that reports have been verified prior to a detailed investigation being authorised</p> <p>If false-positive flags are identified this will mean that the process of updating Active Directory on a regular basis will need to be enhanced</p>	
<p>Further breaches of confidentiality may occur until the full functionality of</p>	<p>Manual audits in place</p>	2	2	4	<p>Damage to corporate reputation and possible financial penalty awarded</p>	2	1	2	<p>Staff will be notified of project via an awareness campaign. This will include reminder of staff</p>

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)	
FairWarning is fully implemented									responsibilities in relation to maintaining confidentiality Staff attend annual IG training which reminds them of their responsibilities in relation to maintaining confidentiality Part of terms and conditions of employment states that a breach of confidentiality is viewed as Gross Misconduct and will be dealt with accordingly. All staff sign up to these terms and conditions. Work

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)	
									with suppliers to ensure full functionality
Nominated end users may not have time to review the reports produced by FairWarning and if this is the case the Trust's overall information risk will not be reduced  Breaches of confidentiality may not be investigated if delegated staff do not have the time and this could lead to fraudulent activity e.g. patient demographics sold onto insurance		2	2	4	Damage to corporate reputation, possible financial penalty awarded and risk of civil action	2	1	2	Staff attend annual IG training which reminds them of their responsibilities in relation to maintaining confidentiality Part of terms and conditions of employment states that a breach of confidentiality is viewed as Gross Misconduct and will be dealt with accordingly. All staff sign up to

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)	
companies, identity fraud etc									these terms and conditions

## 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 our original purpose or we get specific consent for the new purpose.</li> </ul>
<p><b>Principle 3 –</b></p>	<ul style="list-style-type: none"> <li>• We only collect personal data we actually need for our specified purposes.</li> </ul>

<p>Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed</p>	<ul style="list-style-type: none"> <li>• We have sufficient personal data to properly fulfil those purposes.</li> </ul>
<p><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</p>	<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>
<p><b>Principle 5 –</b> Kept no longer than is necessary</p>	<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>
<p><b>Principle 6 –</b> Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage</p>	<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> <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</li> </ul>

	<p>those specified by established frameworks like Cyber Essentials.</p> <ul style="list-style-type: none"><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>
--	--