Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

Data Protection Impact Assessment

Title	Ref number
Transition to InfoFlex Web	

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, a representative from NHIS, 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	
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		
Activity	**IAO**	**Governance**
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		
Activity	**IAO/IAA**	**Governance**
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

Project Title:	**Transition to InfoFlex Web**

Project Description: Describe in sufficient detail for the proposal to be understood
The Trust currently uses InfoFlex desktop as their cancer system. A new development which is required to meet a national project (also incorporated into the 2022/23 planning guidance) involves expanded use of the InfoFlex system - building a Remote Monitoring System (RMS). It has been strongly recommended by Civica (InfoFlex Provider) that the Trust builds the RMS in the web-based InfoFlex version rather than desktop, and this has been the direction of travel for many trusts nationally, therefore the Cancer Team plan to build the RMS in InfoFlex web.

Overview of the proposal: What the project aims to achieve
Patient Stratified Follow-Up (PSFU) is a national project outlined by NHS England/Improvement. The 2022/23 planning guidance highlights that trusts should have fully operational and sustainable PSFU pathways for breast, prostate, colorectal and one other cancer by the end of the first quarter of 2022/23; and two further cancers (one of which should be endometrial) by March 2023. There are many components associated with being able to achieve operational and sustainable PSFU pathways. One of the most significant requirements is a Remote Monitoring System (RMS) where all patients who are having surveillance investigations organised by secondary care should be recorded. The system should record the necessary information to be able to manage the follow-up investigations e.g., when surveillance tests are due, dates they were ordered, and maintaining records of the results. Notes from any contact with patients will also be stored in the RMS. The Trust currently uses InfoFlex as their cancer system, thus cancer tracking, multi-disciplinary team discussions etc. are all captured within this system. Historically within the project, it was agreed that InfoFlex would be the optimum system to be used to build an RMS for each relevant tumour site. Whilst the Trust currently operates the desktop version of InfoFlex, it is strongly recommended by Civica (InfoFlex provider) that RMSs are built within the web-based version, and this has been the direction of travel for many trusts nationally. There are no plans for the desktop version to be decommissioned as yet, but Civica's strategy is to move across to the Web. Remaining with InfoFlex Desktop would mean that any design requests from Civica would be extremely costly as 'off the shelf' designs

are only being made for the web now. The web version is also much more user friendly for staff. The detail contained within this document is therefore related to the transition to InfoFlex web.

Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in DPIA assessment (Include Email Address):	Kathryn Grayson, Cancer Improvement Programme Manager

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Maggie McManus	Deputy COO	Sherwood Forest Hospitals NHS Foundation Trust	14th June 2022
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	13th June 2022
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	13th June 2022
Senior Information Risk Owner	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	26th July 2022
Caldicott Guardian	David Selwyn	Medical Director	Sherwood Forest Hospitals	20th October 2022

			NHS Foundation Trust	
Chief Digital Information Officer	Richard Walker	Chief Digital Information Officer	Sherwood Forest Hospitals NHS Foundation Trust	4th October 2022

Assessment Summary

To be completed by Information Governance

Outcome of Data Protection Impact Assessment:	
1. Project/Implementation is recommended **NOT** to proceed, as significant corporate/customer risks have been identified.	☐
2. Project/Implementation to proceed once identified risks have been mitigated as agreed.	☒
3. Project/Implementation has met required legislative compliance and poses not significant risks. No further action required.	☐

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks:
Summary: Legislative Compliance: Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Article 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity) Article 9(2)(i) allows processing for "ensuring high standards of quality and safety of health care." – which would cover research, audit, service improvement and addressing public health/inequalities **Summary of Risks**: Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management.

Risks

1. Loss of system access - Full system back-up process in place
2. Loss of system data - Full system back-up process in place
3. Leavers' access not removed – InfoFlex team notified of leavers by HR.
4. 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.
5. InfoFlex Web 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
6. Data is accessed inappropriately – individual access is authenticated by Active Directory.
7. Patient safety case outstanding - The patient safety team are aware of this project and have allocated time to review the new functionality

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	**Recommendation Owner:**	**Agreed Deadline for action:**
Information Asset Administrators to ensure InfoFlex Web is added to the information asset register and data flows are mapped and recorded Ensure business continuity plans are in place Account management Standard Operating Procedure generated and implemented, routine audit to take place. Patient safety case to be undertaken. The patient safety team are aware of this project and have allocated time to review the new functionality	IAA	31st October 2022

Stage 1 – Initial Screening Questions

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

Q	Screening question	Y / N	Justification for response
1	Will the project involve the collection of information about individuals?	Y	In order to manage cancer pathways in line with national guidelines, the Trust is required to collect information on cancer patients to ensure they receive the follow-up care they need. The information will include when surveillance investigations/follow-ups are due for patients, any discussions had with the Nursing team about concerns raised, whether a holistic needs assessment has been offered and/or completed with the patient etc. All information collected is required to effectively manage the cancer follow-up pathway.
2	Will the project compel individuals to provide information about themselves?	Y	The same information patients are providing today will be collected in the system.
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Y	From the end of March 2022, there will be a statutory requirement to share this information via the information standard https://digital.nhs.uk/binaries/content/assets/website-assets/isce/dcb1521/1521132019isn.pdf. Data captured within InfoFlex Web will be submitted as part of the Cancer Outcome and Services Dataset (COSD) submission. The information will be shared with: - National Cancer Registration and Analysis Service - East Midlands Cancer Alliance - Nottingham and Nottinghamshire Clinical Commissioning Group

Q	Screening question	Y / N	Justification for response
			The data captured within COSD is made available publicly, therefore patients, other Trusts etc. can all view the results.
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	From the end of March 2022, there will be a statutory requirement to share this information within the COSD submission (as outlined in question 3).
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	The data captured within the RMS will be actively monitored and updated by the Cancer Nurse Specialists as this information will be required to fulfil patients' follow-up care. Demographic information will be fed by CareFlow.
6	Are there security arrangements in place while the information is held?	Y	Only those who have been given access to InfoFlex will be able to view the data. Civica, the supplier of the InfoFlex Web application hold ISO 27001 and Cyber Essentials. Data will be stored on SFH-Infoflex-01.nhis.local which is hosted locally by NHIS.
7	Does the project involve using new technology to the organisation?	N	The web-based system will use existing infrastructure.
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	The information captured within InfoFlex will inform patient pathway management.
If you have answered "Yes" to any of the questions numbered 1-8 please proceed and complete stage 2.			
9	Is a Patient Safety Review required?	Y	13th June 2022 - The patient safety team are aware of this project and have allocated time to review the new functionality

Q	Screening question	Y / N	Justification for response
	DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital		
10	Is a Quality Impact/Technical Security Review required?	Y	Civica has carried out robust reviews of third parties used to deliver the InfoFlex Web service. Third parties used are IBM for the UK Cloud Infrastructure who have many accreditations including ISO 27001 details can be viewed here: https://www.ibm.com/support/pages/ibm-iso-management-system-certifications The optional calendar synchronisation is provided by Cronofy details of their ISO etc. can be found here: https://www.cronofy.com/privacy/ The optional SMS text messaging service is supplied by Twilio, details of their certifications can be found here: https://www.twilio.com/legal/data-protection-addendum https://www.twilio.com/gdpr https://www.twilio.com/legal/privacy/shield Removable media - Civica do not use removable media to transfer data rather SFTP sites are used and set up for specific tasks as required. Remote working - Many Civica employees work remotely and access to Civica systems is via strictly controlled VPN. InfoFlex is accessed via Active Directory. NHIS have reviewed the supplier assurance framework and have not identified any concerns or recommendations

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

Stage 2 – Data Protection Impact Assessment

2.1	What is the change					
	New purpose?	☐	Revised/changed?	☒	Other?	☐
	If Other please specify.					

?2.2.1	What data will be processed?					
	Personal Data:					
	Forename	☒	Surname	☒	Age	☒
	DOB	☒	Gender	☒	Address	☒
	Post Code	☒	NHS No	☒	Hospital No	☒
	Other unique identifier (please specify)					
	Sensitive Personal Data (special categories):					
	Children					☐
	Vulnerable groups					☒
	Racial or ethnic origin					☐
	Political opinion					☐
	Religious Belief					☐
	Trade Union Membership					☐
	Physical or mental health or condition					☒
	Sexual Health					☐
	Criminal offence data					☐
	Other data (please specify)					

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

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	The Remote Monitoring System to be built within InfoFlex Web will enable the following: - Patient data set information to be pulled from CareFlow EPR - Test results to be pulled from local diagnostic IT systems e.g. ICE, Winpath - Storage of key diagnostic and patient history data - Logging of any relevant treatment history during monitoring period, including a log of patient contacts - Setting individual patient range/tolerances for specific tests - Scheduling tests based on user definable follow up schedules - Holding a range of template letters to enable communication of results to patients and GPs by post or electronically - Identifying test results for review, due dates exceeded or test results that exceed tolerance - Providing a summary history and treatment page with test results shown numerically and graphically - Recording the outcome of any event or test - Providing standard and ad hoc reporting and routine monitoring function and be amenable to clinical audit All of the above will enable safe management of cancer patients' follow-up care. Testing of the new system functionality and integration with current Trust systems will be undertaken as part of the design process with Civica.
2.3.1	How will you collect, use, store and delete data?	
	Demographic data on InfoFlex is populated by HL7 messaging from CareFlow. This demographic data is then stored in database Infoflex5_live on server SFH-Infoflex-01.nhis.local which is hosted locally by NHIS. Deleting data will be in line with the Records Management Code of Practice.	

2.3.2	What is the source of the data? (i.e. from data subject, system or other third party)
	Data subject information will be imported from CareFlow EPR. Investigation results will be imported from the relevant systems: - Radiology = KRIS - Pathology = Winpath - Endoscopy = Endobase
2.3.3	How much data will you be collecting and using?
	The minimum amount of information required to manage the patient's pathway.
2.3.4	How often? (for example, monthly, weekly)
	Daily
2.3.5	How long will you keep it? https://www.sfh-tr.nhs.uk/media/12002/isp-101-records-management-code-of-practice-2021.pdf
	Deleting data will be 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
	Stored on SFH-Infoflex-01.nhis.local which is hosted locally by NHIS.
2.3.7	How many individuals are affected?
	All cancer patients. The geographical area for the Trust.
2.3.8	What geographical area does it cover?
	This will be dependent on the patient's home address. The majority of patients live within central Nottinghamshire, however some come from surrounding areas of South Nottinghamshire, Derbyshire and Lincolnshire.

2.4	Who are the Organisations involved in processing (sharing) the data?

	Organisations Name	Data Controller or Data Processor *The **Data Controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.* *The **Data Processor**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.*
	Sherwood Forest Hospitals NHS Foundation Trust	Data Controller
	Civica UK Ltd	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 **supplier and the Trust**	
	Y/N	**If yes the third party will need to complete the following assessment. This will need to be provided in addition to the completion of this proforma. An example of a completed assessment is also provided below** NHIS - Supplier Assurance Framework Supplier Assurance Framework - Example Cloud Assessment.xlsx
		Civica Supplier Assurance Framework
2.5.1	Please describe access and controls in place Account access management Standard Operating Procedure to be completed prior to the implementation of the project https://www.sfh-tr.nhs.uk/media/12007/ig-012-account-management-and-access-policy-2021.pdf Account ManagementSOP Tem Account ManagementSOP Tem	

	SOP.docx			
2.5.2	Please provide a copy of the contract in place			
	KCS Form of Direct Award Y20011 - Sher	Sherwood KCS Contract.pdf - Infoflex		
2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?			
	See Data Protection and GDPR section of the attached KCS Form of Direct Award Y20011 - Sher			
2.5.4	Is the supplier registered with the ICO? Please check the register		Yes	No
			Z5268164	
2.5.5	Has the supplier received ICO Enforcement? Please check the register		Yes	No
				X
2.5.6	Has the supplier received ICO Decision Notice? Please check the register		Yes	No
				X
2.5.7	Has the supplier received an ICO Audit? Please check the register		Yes	No
				X
2.5.8	Has the supplier completed a Data Security and Protection Toolkit, please check the register and provide the following details	Completed: Yes/No	Date submitted	Standard Met/Not Met
		Yes - 8HC47	Published 17th February 2022	Standards Met

<table>
<tr><td rowspan="5">2.5.9</td><td colspan="3">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</td></tr>
<tr><td></td><td>Yes</td><td>No</td></tr>
<tr><td>Cyber Essentials Plus</td><td></td><td> 
Cyber Essentials Certificate - Civica UK.</td></tr>
<tr><td>ISO 15489 Records Management</td><td></td><td>X</td></tr>
<tr><td>ISO 27001 Information Security Standards</td><td> 
27001 - Civica HQ with Annex (1).pdf</td><td></td></tr>
<tr><td></td><td>ISO 9001 Quality Management Systems</td><td> 
9001 - Civica HQ with Annex (1).pdf</td><td></td></tr>
<tr><td>2.5.10</td><td colspan="3">Is the data held outside of the UK ie Europe, USA, Ireland? If yes please include the country</td></tr>
<tr><td rowspan="2"></td><td colspan="2">Yes</td><td>No</td></tr>
<tr><td colspan="2"></td><td>X</td></tr>
<tr><td></td><td colspan="3">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</td></tr>
<tr><td></td><td colspan="3">Not applicable</td></tr>
<tr><td rowspan="3">2.6</td><td colspan="3">Will this information be shared outside the organisations listed above?</td></tr>
<tr><td>Y/N</td><td colspan="2">if answered Yes please describe organisation/s and geographic location</td></tr>
<tr><td>Y</td><td colspan="2">From the end of March 2022, there will be a statutory requirement (information standard) to share this information.

Data captured within InfoFlex Web will be submitted as part of the Cancer Outcome and Services Dataset (COSD) submission.

The information will be shared with:</td></tr>
</table>

		- National Cancer Registration and Analysis Service - East Midlands Cancer Alliance - Nottingham and Nottinghamshire Clinical Commissioning Group The data captured within COSD is made available publicly, therefore patients, other Trusts etc. can all view the results.				
2.7	Does the work involve employing contractors external to the Organisation?					
	Y/N	If **Yes**, provide a copy of the confidentiality agreement or contract?				
	Y	See confidentiality section of the attached KCS Form of Direct Award Y20011 - Sher				
2.8	Has a data flow mapping exercise been undertaken?					
	Y/N	If **Yes**, 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					
	Infoflex Information Flows.png					
2.9	What format is the data?					
	Electronic	☒	Paper	☐	Other (Please describe)	Click here to enter text.
2.10	Is there an ability to audit access to the information?					
	Y/N	Please describe if answered **Yes.** If **NO** what contingencies are in place to prevent misuse?				
	Y	InfoFlex has a built-in audit tool which enables auditing of user activity. Information Development Team have also developed a Qlik Dashboard to undertake auditing.				

2.11	Does the system involve new links with personal data held in other systems or have existing links been significantly changed?	
	Y/N	Please describe if answered **Yes**
	Y	The Trust are adding two additional links, one for Endoscopy reports, and another for PACs.

2.12	How will the information be kept up to date and checked for accuracy and completeness? (data quality) How will you ensure data minimisation?	
	The data captured within the RMS will be actively monitored and updated by the Cancer Nurse Specialists as this information will be required to fulfil patients' follow-up care. Demographic information will be fed by CareFlow EPR.	
2.13	Who will have access to the information? (list individuals or staff groups)	
	Cancer Nurse Specialists MDT Coordinators Cancer Management Team Tumour Site Clinicians Business Intelligence Team Information Team	
2.14.1	What security measures have been implemented to secure access?	
	Active Directory (Window's username and password)	☒
	Username and password	☐
	Smartcard	☐
	Key locked filing cabinet/room	☐
	Hard/soft Token (VPN) Access	☒

	Restricted Access to Network Files (shared drive)	☐
	Has information been anonymised?	☐
	Has information been pseudonymised?	☐
	Is information fully identifiable?	☒
	Other (provide detail below)	☐
	VPN access for remote working. Access to the system is via individual Window's accounts so no separate username and password required to access the system	
2.14.2	What physical security measures have been implemented to secure access? ie swipe cards, digilock	
	Data is held on Trust servers and access to the server rooms is tightly controlled and monitored by CCTV	
2.15	Will the data be stored on Trust servers	
	Yes	No
	X	

2.16	Please state by which method the information will be transferred?			
	Email (not NHS.net)	☐	NHS.net	☐
	Website Access (internet or intranet)	☒	Wireless Network (Wi-Fi)	☐
	Secure Courier	☐	Staff delivered by hand	☐
	Post (internal)	☐	Post (external)	☐
	Telephone	☐	SMS	☐
	Other	☐	please specify below	☐

	HL7 messaging from CareFlow, Winpath and Endobase into InfoFlex Submissions via Website Access	
2.17	Are disaster recovery and business contingency plans in place for the information? What types of backups are undertaken i.e. full, differential or incremental?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
		We have a business continuity plan if the service was unavailable. The department would default back to the current practice and access the information manually Standard NHIS protocol SSRS reports for PTL to support tracking Paper forms for MDTs

2.18	Has staff training been proposed or undertaken and did this include confidentiality and security topics areas?	
	Y/N	Please describe if answered **Yes**
	Y	Internal training SOPs

2.19	Will reports be produced?	
	Will reports contain personal/sensitive personal or business confidential information?	Yes
	Who will be able to run reports?	Analyst team Cancer team
	Who will receive the reports and will they be published?	From the end of March 2022, there will be a statutory requirement (information standard) to

		share this information. Data captured within InfoFlex Web will be submitted as part of the Cancer Outcome and Services Dataset (COSD) submission. The information will be shared with: - National Cancer Registration and Analysis Service - East Midlands Cancer Alliance - Nottingham and Nottinghamshire Clinical Commissioning Group The data captured within COSD is made available publicly, therefore patients, other Trusts etc. can

		all view the results.
2.20	If this new/revised function should stop, are there plans in place for how the information will be **retained / archived/ transferred or disposed of?**	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The data will be transferred from Civica to the Trust or the new supplier. The data will then be securely destroyed at Civica.
2.21	Is consent required for processing of personal data?	
	Y/N	Please describe if answered **Yes**
	N	Direct healthcare and legal basis under the Health and Social Care Act
		If **No**, list the reason for not gaining consent e.g. relying on an existing agreement, consent is implied, the project has s251 approval or other legal basis?
		Part of our statutory duties under GDPR 6(1)(e) public interest or public duty, and Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
2.22	Will individuals be informed about the proposed uses and share of their personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The Trust's privacy notice is here https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/
2.23	Is there a process in place to remove personal data if data subject refuses/removes consent	

	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
		N/A – Direct Healthcare
2.24	How much control will they have? Would they expect you to use their data in this way?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
		N/A – Direct Healthcare
2.25	Are arrangements in place for recognising and responding to requests for access to personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	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: Sherwood Forest Hospitals (sfh-tr.nhs.uk)
2.26	Who are the Information Asset Owner(s) and Administrator(s)?	
	IAO	Maggie McManus
	IAA	Sam Owen
	System Administrators	There are InfoFlex users who are added to the 'Administrator' group in InfoFlex.
2.27	How is the data secured in transit and at rest? Eg encryption, port control number	
	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.	
2.28	Has the impact to other NHIS systems/processes been considered and appropriate SBU's consulted and in particular technical security?	

	Y/N	Please describe if answered **Yes.** Please state what checks were undertaken if response is answered **No.** DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital
	Y	13th June 2022 - The patient safety team are aware of this project and have allocated time to review the new functionality
2.29	Are there any current issues of public concern that you should factor in?	
	Y/N	Please describe if answered **Yes.**
	N	
2.30	What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?	
	To improve the follow-up management of cancer patients.	
2.31	Consider how to consult with relevant stakeholders: • Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. • Who else do you need to involve within your organisation? • Do you need to ask your processors to assist?	
	Kathryn Grayson presented this document to the Information Governance working group for consultation. Key stakeholders at the IG Working Group include: • The Trust Risk Manager • Clinical Lead for ICT • DPO/IG Manager • Information Security Officer • Divisional Representatives from the Trust RMS helps to manage follow-up investigations and allows for any contacts to be recorded.	

2.32	What is your lawful basis for processing? (please see Appendix 10 Information Sharing Protocol for further information). **Consent is usually the last basis to rely on**

	Legal basis: patients **Personal data i.e. name, address** 6(1)(a) the patient has given consent 6(1)(c) necessary for legal obligations 6(1)(e) public interest or public duty 6(3) the above supported by Member State law (UK legislation as applicable to circumstances) **Sensitive personal data (special category)** 9(2)(a) the patient has given explicit consent 9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc.) 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity). 9(2)(i) allows processing for "ensuring high standards of quality and safety of health care." – which would cover research, audit, service improvement and addressing public health/inequalities. 9(2)(j) (together with Article 89 and relevant recitals) relates to archiving, statistical analysis and research. **Legal basis: staff** – please review Appendix 10 Information Sharing Protocol for further information).
	The Trust's lawful basis for processing personal and special categories of personal data are: 1. 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. 2. Article 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 3. Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the

	employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services. Supplier 1. 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. 2. Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
2.33	What information will you give individuals about the processing? (This information will be added to the Trust's Patient Privacy Notice and Staff Privacy Notice by the Information Governance Team)
	This DPIA will be published once finalised. The Trust's privacy notice has been updated.

2.34	What measures do you take to ensure processors comply?
	The Trust and Civica have a contract in place and this will be reviewed on a regular basis.
2.35	How will you prevent function creep? Manage lifecycle of system/process
	Civica will only ever process the Trust's data as per explicit agreement with the Trust The Trust and Civica have a contract in place where roles and responsibilities are defined. To prevent function creep, processing activity will be carried out on behalf of the Trust by Civica that is agreed to. The Service Agreement provides explicit information on processing activity provided by Civica as part of offering the InfoFlex Web service. As data controller, the Trust has full responsibility for ensuring health care professionals accessing the system utilise it appropriately.

Stage - 3 Risk Template

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

Completed by	Gina Robinson	Role:	Information Security Officer	Date completed: 19th 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)**	
Loss of system access	Full system back-up process in place	2	2	4	System back-up not present	2	2	4	Manual input, business continuity plan to be used
Loss of system data	Full system back-up process in place	3	2	6	System back-up not present	2	2	4	Manual input, business continuity plan to be used
Leavers' access not removed	InfoFlex team notified of leavers by HR monthly report	3	1	3	Ensure access is managed and leavers list is received and actioned	3	1	**3**	Ensure access is managed and leavers list is received and actioned

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)**	
Business continuity plans in each area, do these exist and is there a template for recording if InfoFlex Web goes down.	Business Continuity plan for the InfoFlex system is in place	3	1	3	Business continuity plan in place.	3	1	**3**	Business continuity plan reviewed annually.
If the system is not recorded on the information asset register, the system may not be brought back online in response to a cyber attack	In the Trust we have a business continuity plan if the service was unavailable.	2	2	4	InfoFlex Web will need to be added to the divisional information asset register and recorded as part of the annual IAO returns to the SIRO	2	1	**2**	InfoFlex Web will need to be added to the divisional information asset register and recorded as part of the annual IAO returns to the SIRO
Data is accessed inappropriately.	Active Directory username and password controls in place. Privileged access only.	2	2	4	Access data inappropriately	2	1	**2**	Routine audits

Risk Scoring Matrix.pdf

Stage – 4 Legal Compliance

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

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

	our original purpose or we get specific consent for the new purpose.
Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed	• We only collect personal data we actually need for our specified purposes. • We have sufficient personal data to properly fulfil those purposes.
Principle 4 – Personal data shall be Accurate and, where necessary, kept up to date, having regard to the purposes for which they are processed, are erased or rectified without delay	• We ensure the accuracy of any personal data we create. • We have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data. • We have a process in place to identify when we need to keep the data updated to properly fulfil our purpose, and we update it as necessary. • If we need to keep a record of a mistake, we clearly identify it as a mistake. • Our records clearly identify any matters of opinion, and where appropriate whose opinion it is and any relevant changes to the underlying facts. • We comply with the individual's right to rectification and carefully consider any challenges to the accuracy of the personal data. • As a matter of good practice, we keep a note of any challenges to the accuracy of the personal data
Principle 5 – Kept no longer than is necessary	• We know what personal data we hold and why we need it. • We carefully consider and can justify how long we keep personal data. • We have a policy with standard retention periods, however due to the Goddard Inquiry no destruction or deletion of patient records is to take place until further notice.
Principle 6 – Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage	• We undertake an analysis of the risks presented by our processing, and use this to assess the appropriate level of security we need to put in place.

	• We have an information security policy (or equivalent) and take steps to make sure the policy is implemented. We have put in place technical controls such as those specified by established frameworks like Cyber Essentials. • We use encryption. • We understand the requirements of confidentiality, integrity and availability for the personal data we process. • We make sure that we can restore access to personal data in the event of any incidents, such as by establishing an appropriate backup process. • We conduct regular testing and reviews of our measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement. • We implement measures that adhere to an approved code of conduct or certification mechanism. • We ensure that any data processor we use also implements appropriate technical and organisational measures.