Healthier Communities, Outstanding Care

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

Data Protection Impact Assessment

Title	Ref number
Logex Costing System	

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:	**Logex Costing System (Patient Level Information Costing System ((PLICS)**

Project Description: Describe in sufficient detail for the proposal to be understood
At the end of 2020 we were using a costing system supplied by Prodacapo. Prodacapo had recently been acquired by a company called Logex. Logex prices were considerably higher than Prodacapo and we took the opportunity to assess other suppliers in the market and in January 2021 we changed supplier to Assista and implemented the Assista Monitor costing system on a 3-year contract. Subsequently Logex have acquired Assista (September 2021), and we now have to implement the Logex costing system as the Assista system is going to be discontinued.

Overview of the proposal: What the project aims to achieve
Replace current on-premises Assista Monitor Costing Solution by new hosted costing technology.

Implementing Organisation:	LOGEX Group (formerly Prodacapo)

Staff involved in DPIA assessment (Include Email Address):	Greg Sheriston, the Trust

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Jennifer Leah	Deputy Chief Finance Officer	Sherwood Forest Hospitals NHS Foundation Trust	14th February 2022

Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	3rd February 2022
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	1st February 2022
Senior Information Risk Owner	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	14th February 2022
Caldicott Guardian	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	20th June 2022
Chief Clinical Information Officer	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	20th June 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 no 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)

Summary of Risks:
Cyber security and Information Asset Management

Risks

1. **Loss of data on supplier cloud server meaning reports and information cannot be provided to end users**. Full system back-up process in place
2. **Inappropriate access to data which may lead to inaccurate reporting.** Only the costing team require access and there are strict access control policies. The data is only accessible from the Trust network and requires username and password.
3. **Inappropriate disclosure that may lead to inaccurate reporting**. Secure data transfer between systems mitigates this risk (TLS 1.2).

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	**Recommendation Owner:**	**Agreed Deadline for action:**
Currently passwords for administrator accounts must be changed at least every 48 months or immediately if a user with knowledge of the password leaves the Trust or no longer requires access to the account based on their role. Consider administrator accounts password changes to 12 months instead of 48 months seems along time to have a password for. If this is to remain at 48 months would need to be captured as a risk.	Greg Sheriston	31st March 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	Yes, but pseudonymised data is shared with LOGEX and the Trust is the only party that holds the key. LOGEX processes data using this replacement ID and sends the outcomes of processing back to Trust. The Trust is then able to translate (reidentify) ID's to original patient ID's.
2	Will the project compel individuals to provide information about themselves?	N	
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	N	
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N	
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	Data that is processed is required for regulatory driven processing. The Data Processing Agreement clearly stipulates which data elements are required. No additional data is collected. An extensive data validation process is applied after each data delivery, based on the agreement made between the Trust and LOGEX.
6	Are there security arrangements in	Y	Pseudonymisation of data is one of the core security elements: Data is not to be related to individual persons without the key for

Q	Screening question	Y/N	Justification for response
	place while the information is held?		reidentifying which is held by the Trust. Secondly data is stored in well protected market standard Cloud environments (Microsoft Azure) including appropriate back-up, security and access policies which meets market security standards. LOGEX is yearly ISO/NEN and ISAE 3402 type II audited on all of these aspects.
7	Does the project involve using new technology to the organisation?	Y	New costing technology concerns an upgrade to existing costing technology which is already implemented elsewhere. The upgraded technology has been applied and proven in multiple countries (Netherlands, Sweden, Finland, Norway). Limited changes have been made during implementation to make it fit for UK purpose. Changes made primarily include country specific alterations, such as localization, codes and NHSI regulation.
8	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	N	
If you have answered "Yes" to any of the questions numbered 1-8 please proceed and complete stage 2.			
9	Is a Patient Safety Review required? DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital	N	
10	Is a Quality Impact/Technical Security Review required?	N	The data is uploaded via Data Connect, which is a secured web portal, so data can also be transferred by the Trust without the need of a consultant. For web access we use TLS 1.2 or higher with strong cypher suites as defined by the National Institute of Standards and

Q	Screening question	Y/N	Justification for response
			Technology (NIST) guidelines for Transport Layer Security (TLS) implementations. For Virtual Private Networks (VPN) connections only strong cryptographic controls as defined by the National Institute of Standards and Technology (NIST) guidelines for cryptographic algorithms and key lengths. Microsoft is ISO27001 compliant https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001

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)		The patient ID (NHS number) is pseudonymised			
	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 uploaded via Data Connect, which is a secured web portal, so data can also be transferred by the Trust without the need of a consultant. For web access we use TLS 1.2 or higher with strong cypher suites as defined by the National Institute of Standards and Technology (NIST) guidelines for Transport Layer Security (TLS) implementations. For Virtual Private Networks (VPN) connections only strong cryptographic controls as defined by the National Institute of Standards and Technology (NIST) guidelines for cryptographic algorithms and key lengths.					

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	To provide Patient Level Costing System (PLICS) to the Trust and the benefits therein. To produce mandated annual PLICS returns to NHSI/E
2.3.1	How will you collect, use, store and delete data?	
	Collect and transfer data The data is uploaded via Data Connect, which is a secured web portal, so data can also be transferred by the Trust without the need of a consultant. For web access we use TLS 1.2 or higher with strong cypher suites as defined by the National Institute of Standards and Technology (NIST) guidelines for Transport Layer Security (TLS) implementations. For Virtual Private Networks (VPN) connections only strong cryptographic controls as defined by the National Institute of Standards and Technology (NIST) guidelines for cryptographic algorithms and key lengths. **Store data** LOGEX applications are hosted on resilient Microsoft Azure infrastructure with extremely high SLA. The Azure SLA (For example single instances virtual machines have an availability of 99.9%) fits very well in LOGEX SLA. In the case of disaster recovery (e.g. data centre crashes) then we always failover to another Azure location in the UK **Delete data**	

	Upon request of the client or after maximum of five years after year-closing data will be deleted.
2.3.2	What is the source of the data? (i.e. from data subject, system or other third party)
	The Trusts Patient Administration System (CareFlow EPR) is the main source of data. Supplemented by other systems, e.g. Pathology, Radiology.
2.3.3	How much data will you be collecting and using?
	It regards Trusts financial data and pseudonymised patient data (see annex 1 in attached DPA) for all patients administered by the Trust during a certain time period (e.g. last year).
2.3.4	How often? (for example monthly, weekly)
	Yearly (and in some cases quarterly or monthly)
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
	Five years maximum. Trust can review data to 5 years back (for comparison purposes). Data will be deleted after 5 years or when Trust explicitly request deletion.
2.3.6	Where will the data be stored? i.e. CareFlow, Shared Drive, offsite storage
	LOGEX applications are hosted on resilient Microsoft Azure infrastructure with extremely high SLA. The Azure SLA (For example single instances virtual machines have an availability of 99.9%) fits very well in LOGEX SLA. In the case of disaster recovery (e.g. data centre crashes) failover is activated to another Azure location in the UK. 20201012 LOGEX Costing Solution - Fre
2.3.7	How many individuals are affected?
	N/A: It regards processing of patient data stored at Trust for regulatory purposes.
2.3.8	What geographical area does it cover?
	UK Only. Most data will be from Nottinghamshire and Derbyshire, but a small number of patients will be from other areas of the UK.

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

	Organisations Name	Data Controller or Data Processor *The **Data Controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.* *The **Data Processor**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.*
	Sherwood Forest Hospitals NHS Foundation Trust	Data Controller
	LOGEX Healthcare analytics Ltd. (formerly Prodacapo)	Data Processor
	Microsoft	Sub 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
	N	As the Trust extracts and uploads the data to the LOGEX Online environment, there is no access to existing Trust network or systems. Microsoft is ISO27001 compliant https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001
2.5.1	Please describe access and controls in place 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	

	https://www.sfh-tr.nhs.uk/media/12008/ig-0121-account-management-sop-template-sept-21.pdf			
	Please see attached LOGEX ISO certification  Account Management - Logex  IS 590552 - 1.pdf			
2.5.2	Please provide a copy of the contract in place			
	Please see attached current Prodacapo contract and new Data Processing Agreement. Annex 1 is the current DPA and includes reference to health care data  Data Processing Agreement for Sherw  Template English data processing agree  Annex 1 - Data Processing Agreemen			
2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?			
	Yes, part of the Data Processing Agreement.			
2.5.4	Is the supplier registered with the ICO? Please check the register	Yes	No	
		x		
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	10/06/2021	Met (Exceeded)

2.5.9	Can the supplier demonstrate compliance with any of the following standards? If YES please provide further information e.g. date achieved and a copy of the certificates		
		Yes	No
	Cyber Essentials Plus		x
	ISO 15489 Records Management		x
	ISO 27001 Information Security Standards	FAQ_annex._ISO_-_LOGEX_ISO27001_cert Microsoft https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001	
	ISO 9001 Quality Management Systems	Microsoft https://docs.microsoft.com/en-us/azure/compliance/offerings/offering-iso-9001?toc=/compliance/regulatory/toc.json&bc=/compliance/regulatory/breadcrumb/toc.json	
2.5.10	Is the data held outside of the UK ie Europe, USA, Ireland? If yes please include the country		
	Yes		No
			No, UK South
	If yes we need to seek assurance that the data will continue to flow post Brexit 31.12.2020, provide further detail below from the supplier		
	Not applicable		
2.6	Will this information be shared outside the organisations listed above?		
	Y/N	if answered **Yes** please describe organisation/s and geographic location	
	Y	NHSI/E	

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	Logex employees only				
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					
	 Annex1_UK.docx  Finance Data Flow Map Jan 22 - With Co					
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	LOGEX has a policy for external accounts (access to applications on LOGEX Online) and applies a user management system for the management and monitoring of authorizations. Management Team evaluates the policy on a periodic basis and approves the latest version. LOGEX requires an IP-restriction for users of the Financial Control platform. This means users can only log in from the hospital network. Users of LOGEX Online have a personal username and password. Password requirements meet the current best practices and need to contain at least 8 characters, at least 1 capital and at least 1 number.				
2.11	Does the system involve new links with personal data held in other systems or have existing links been significantly changed?					

	Y/N	Please describe if answered **Yes**
	N	

2.12	How will the information be kept up to date and checked for accuracy and completeness? (data quality) How will you ensure data minimisation?	
	We run a validation report on every delivery. We check: - Fullness of data against previous periods - Consistency of data (can we link all encounters to patients, etc.) - Correctness of data: Only those data elements stated in the DPA are accepted.	
2.13	Who will have access to the information? (list individuals or staff groups)	
	Finance Team and 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)	☒

	LOGEX has a policy for external accounts (access to applications on LOGEX Online) and applies a user management system for the management and monitoring of authorizations. LOGEX requires an IP-restriction for users of the Financial Control platform. This means users can only log in from the hospital network. Users of LOGEX Online have a personal username and password. Password requirements meet the current best practices and need to contain at least 8 characters, at least 1 capital and at least 1 number.			
2.14.2	What physical security measures have been implemented to secure access? ie swipe cards, digilock			
	Microsoft https://docs.microsoft.com/en-us/compliance/regulatory/offering-iso-27001			
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	☒
	Data will be uploaded via secure portal (LOGEX Online). User can only connect to secure portal from Trust network (or via VPN connection).			

	For web access we use TLS 1.2 or higher with strong cypher suites as defined by the National Institute of Standards and Technology (NIST) guidelines for Transport Layer Security (TLS) implementations. For Virtual Private Networks (VPN) connections only strong cryptographic controls as defined by the National Institute of Standards and Technology (NIST) guidelines for cryptographic algorithms and key lengths.	
2.17	Are disaster recovery and business contingency plans in place for the information? What types of backups are undertaken i.e. full, differential or incremental?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	LOGEX applications are hosted on resilient Microsoft Azure infrastructure with extremely high SLA. The Azure SLA (For example single instances virtual machines have an availability of 99.9%) fits very well in LOGEX SLA. In the case of disaster recovery (e.g. data center crashes) then we always failover to another Azure location in the UK LOGEX has internal control objectives that provide reasonable assurance the operational management of its ICT environment is taking place in a reliable and controllable manner. - LOGEX backs up the internal and external environments in accordance with a backup schedule. Backups of production environments are stored in a physically different location than the location of the actual production environments. - LOGEX monitors back-ups to determine whether the back-ups of internal and external environments have failed or whether components are non-accessible. The back-up software sends automatic emails to the IT Service Provider and LOGEX about the status of the executed backup (successful: yes/no). Possible required actions are logged in the ticketing system of the IT Service Provider. From September 2019 onwards automatic emails to the IT Service Provider and LOGEX will only be send for failed backups.

		Full and differential back-ups are made such that no to very limited changes can be lost. Over the past 10 years we never had the experience of any loss of data. In the Trust we have a business continuity plan if the service was unavailable.
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	As part of the upgrade the required training for staff members of the Trust will be provided. Given the staff of the Trust is currently working with an existing version of the Costing Solution they are aware of confidentiality and security topics. In the new Solution only pseudonymised data is being processed which reduces confidentiality risks.
2.19	Will reports be produced?	
	Will reports contain personal/sensitive personal or business confidential information?	Yes, will only contain aggregated data on department, speciality, diagnose level etc. No personal data. Potentially business confidential data when compared to benchmark
	Who will be able to run reports?	LOGEX will create reports based on request Trust.
	Who will receive the reports and will they be published?	Reports will be distributed by Trust To interested parties (e.g. consultants, DGMs, AGMs, PMO)
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	In case of termination of the agreement all data stored at LOGEX Group will be removed, including back-ups. All existing reports will be shared with Trust.
2.21	Is consent required for processing of personal data?	
	Y/N	Please describe if answered **Yes**
	N	
		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?
		Processing this data for Trust is considered to be common practice for a Trust, as such no explicit information is shared with patients. Please note: There is no change in types of data being processed, nor the reasons for processing. The only thing effectively changing is the method of processing (being the technical steps applied during processing). 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.**
		The Trust's privacy notice is here https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/ The following information will be added to the website: **Patient Level Information Costing System (PLICS)**

		We use anonymised data from the trusts clinical systems to create a detailed model of the trusts clinical services. The PLICS model permits the trust to easily analyse activity and costs, the use of resources, and the efficiency of services. This information enables better decision making and enables more effective use of finite resources. The data is also used by NHSE/I to centrally monitor resources, to aid in the creation of the 'model hospital' and inform contracting decisions.
2.23	Is there a process in place to remove personal data if data subject refuses/removes consent	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	Trust is Controller and thus should instruct LOGEX (being the Processor) in case of an applicable deletion requests. However, given the type of data processed consent is not expected to be the legitimate basis for processing and thus this would be limitedly applicable.
2.24	How much control will they have? Would they expect you to use their data in this way?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	Trust is Controller and thus should instruct LOGEX (being the Processor) in case of an applicable deletion requests. However, given the type of data processed consent is not expected to be the legitimate basis for processing and thus this would be limitedly applicable.
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	Trust is Controller and thus should instruct LOGEX (being the Processor) in case of an applicable access requests. 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	Jennifer Leah
	IAA	Greg Sheriston
	System Administrators	Greg Sheriston, Nicola Stewart
2.27	How is the data secured in transit and at rest? Eg encryption, port control number	
	Secure data transfer between systems (TLS 1.2).	
2.28	Has the impact to other NHIS systems/processes been considered and appropriate SBU's consulted and in particular technical security?	
	Y/N	Please describe if answered **Yes.** Please state what checks were undertaken if response is answered **No.**
	N	Not relevant as the Trust extracts and uploads the data to the LOGEX Online environment, there is no access or connection to existing Trust network or systems.
2.29	Are there any current issues of public concern that you should factor in?	
	Y/N	Please describe if answered **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?	
	The Trust aims to make more effective use of costing information and leverage to new uses within the Trust to facilitate better and affordable healthcare. Impact on individuals is deemed minimal, as it is part of regular business optimisation processes.	
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?
	Greg Sheriston presented this document to the Information Governance working group for consultation.

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).

	Processing of data by the Trust occurs on basis of the provisioning of direct care. Trust is continuously seeking for optimisation of health care process, finding the optimum of high-quality health care provisioning against lowest possible costs. 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). LOGEX processes data to support in mandatory PLICS.
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 following information has been added to the patient privacy notice: **Patient Level Information Costing System (PLICS)** We use anonymised data from the Trusts clinical systems to create a detailed model of the Trusts clinical services. The PLICS model allows the Trust to easily analyse activity and costs, the use of resources, and the efficiency of services. This information enables better decision making and enables more effective use of finite resources. The data is also used by NHS England and Improvement to centrally monitor resources, to aid in the creation of the 'model hospital' and inform contracting decisions.

2.34	What measures do you take to ensure processors comply?
	The Trust has a contract in place with the supplier
2.35	How will you prevent function creep? Manage lifecycle of system/process
	Trust holds control over the data via the self-extraction and sharing. LOGEX only receives those data required for provisioning of in DPA confirmed service. Contractual arrangements explicitly stipulate allowed use of data.

Stage - 3 Risk Template

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

Completed by	Greg Sheriston (Neil Wilkinson)	Role:	Costing Accountant	Date completed: January 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 data on supplier cloud server meaning reports and information cannot be provided to end users.	The supplier has full & differential backup processes (Microsoft Azure), storing data separate to production.	3	1	3		3	1	3	n/a
Inappropriate access to data which may lead to inaccurate reporting	Only the costing team require access and there are strict access control policies. The data is only accessible from the Trust network and requires username and password.	3	1	3		3	1	3	n/a
Inappropriate disclosure that may lead to inaccurate reporting	Secure data transfer between systems mitigates this risk (TLS 1.2)	2	1	2		2	1	2	n/a

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.