Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

Data Protection Impact Assessment

Title	Ref number
Datix upgrade to DatixCloudIQ	

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:	**Datix upgrade to DatixCloudIQ**

Project Description: Describe in sufficient detail for the proposal to be understood
Datix upgrade to DatixCloudIQ version, including the addition of a mortality review module.

Overview of the proposal: What the project aims to achieve
Installation of the latest version of Datix to allow improved functionality, analytics and incident reporting, particularly relating to mortality reviews and Structured Judgement Reviews. This would provide a more robust governance process and assurance that all elements of quality of care and patient experience are triangulated. The Datix system and data would be held on an off-site server managed and maintained by the system supplier, RLDatix, ensuring that system fixes and upgrades are performed promptly.

Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in DPIA assessment (Include Email Address):	Neil Wilkinson Angela Farrands

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	7th December 2021
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	3rd December 2021

Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	30th November 2021
Senior Information Risk Owner	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	7th December 2021
Caldicott Guardian	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	9th December 2021
Chief Clinical Information Officer	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	9th December 2021

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 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 - Datix system team notified of leavers by HR. Changes to user roles reviewed monthly via a Trust e-form report
4. Business continuity plans in each area, users of each module have business continuity plans for their areas/departments

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	**Recommendation Owner:**	**Agreed Deadline for action:**
User access and permissions SOP to be reviewed to ensure appropriate for cloud system access	Angela Farrands	31/01/2021
If the interface to pull data from CareFlow EPR is to be incorporated the DPIA will need to be reviewed.	Neil Wilkinson	TBC if interface is incorporated

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	No change to current data collection
2	Will the project compel individuals to provide information about themselves?	N	
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Y	Data currently held on a Trust server will be on a server managed by RLDatix
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	A new mortality module will be used, although no additional data will be collected. Potential to use an interface to pull in data from CareFlow EPR to assist in triggering mortality reviews
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	Full incident review process in place Risks reviewed on a periodic basis Legal and Patient Experience modules maintained by the respective departments
6	Are there security arrangements in place while the information is held?	Y	RLDatix Security Assurance Framework in place
7	Does the project involve using new technology to the organisation?	N	
8	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	Y	Incident investigations may result in staff disciplinary action Safeguarding incident investigations may result in referrals to external safeguarding organisations
If you have answered "Yes" to any of the questions numbered 1-8 please proceed and complete stage 2.			
9	Is a Patient Safety Review required?	N	22.09.2021 - NHIS have reviewed and a patient safety test is not required

Q	Screening question	Y/N	Justification for response
10	Is a Quality Impact/Technical Security Review required?		The IG team have reviewed the DCIQ Security Assurance Framework and have not identified any concerns or recommendations DCIQ Security Assurance Framework

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)		Overseas patients			

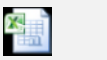
2.2.2	Is the data?					
	Identifiable?	☒	Pseudonymised?	☐	Anonymised?	☐
	If the data is pseudonymised please describe the technical controls in place ie pseudonymised data provided to a third party and the 'key' for re-identification to be retained by the Trust. Also describe how the data will be transferred ie using HL7					

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	Incident report data used to investigate the incident

2.3.1	How will you collect, use, store and delete data?
	Incidents: data input by incident reporter and investigator Risks: data input by risk owners/administrators Legal (including Access to Health Records) and Patient Experience: data input by department staff Data will be deleted according to the Retention & Destruction Policy, although most information is currently kept in line with public and statutory inquiries e.g The Independent Inquiry into Child Sexual Abuse, The Infected Blood Inquiry and the Covid Inquiry.
2.3.2	What is the source of the data? (i.e. from data subject, system or other third party)
	Incidents: from data subject and/or incident reporter and investigator Risks: data input by risk owners/administrators Legal (including Access to Health Records) and Patient Experience: data input by department staff
2.3.3	How much data will you be collecting and using?
	Difficult to quantify – approx. 12,000 incidents reported per year
2.3.4	How often? (for example monthly, weekly)
	Daily.
2.3.5	How long will you keep it?

	 NHSX_Records_Management_Code_of_Prac
	Currently there is not any data on the DatixCloudIQ system. Details of on-going risks will need to be added to DatixCloudIQ, with legacy data deleted at the appropriate time. The Trust is not planning to transfer any data from the old system for incidents, legal, RFI and patient experience. Existing records for these will be closed/completed on the Datix web system (current system) and deleted at the appropriate time. The Trust has not deleted any data for some time because of the complexities of determining which would need to be retained for various Public Inquiries.
2.3.6	Where will the data be stored? i.e. CareFlow EPR, Shared Drive, offsite storage
	DatixCloudIQ is hosted at Tier IV data centres in the UK and adheres to the data security policies, programmes, laws, and procedures of the UK. Certified for storing data within regulated industries they meet the standards of SSAE-16, PCI DSS, and ISO 27001. Application infrastructure is housed in a private isolated network, which prevents it from being directly accessed from the public internet. Within the data centre, DatixCloudIQ data is logically separated between customers; the data and functions among its tenants remain absolutely separate. Data centre facilities are powered by redundant power, each with their own UPS and backup generators.
2.3.7	How many individuals are affected?
	Difficult to quantify – approx. 12,000 incidents reported per year
2.3.8	What geographical area does it cover?
	Predominantly Ashfield, Mansfield, Sherwood, Newark, and Derbyshire but may involve overseas patients

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
	RLDatix	Data Processor

2.5	If we have identified a supplier in 2.4, the following questions for 2.5 and 2.6 will need to be answered by the supplier and the Trust	
	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
	Y	 DCIQ Security Assurance Framework **Penetration Testing** RLDatix uses third-party security experts as part of a risk and compliance framework to run complete penetration tests for exploitable application vulnerabilities, software vulnerabilities, escalation of privileges, prospective access to sensitive data, access scope limitation, and isolation. The security experts are rotated every two years, enabling RLDatix to ensure excellent coverage, evaluate the attack surface, and re-affirm the security baseline.

		Patching Automatic security patching is enabled across the entire RLDatix infrastructure and occurs on a daily basis. **Vulnerability Management** RLDatix has several practices in place to identify and mitigate vulnerability, such as penetration testing that is executed at least once a year or during large upgrades/changes in software. We are currently rolling out an Alert Logic solution to extend our event monitoring, log management, and vulnerability management. Alert Logic scans, monitors and assesses the system 24/7 to detect threats and risks before they cause real damage. This includes: • Active scanning of all components for known vulnerabilities (Automated testing) • Active scanning of Cloud configuration for any configurations that do not meet best practice • Continuous event log collection and monitoring to demonstrate regulatory compliance • Intrusion Detection System (ID S) • Web Application Firewall (WAF) Alert Logic delivers on best practices for PCI DSS Compliance, H IPAA H ITECH, GD PR, Sarbanes-Oxley (SOX), SOC 2 Compliance, NIST, ISO, COBIT, and other mandates. For more information, visit https://www.alertlogic.com/managed-detection-and-response/professional/. The IG team have reviewed the DCIQ Security Assurance Framework and have not identified any concerns or recommendations.
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	
	Incidents can be input by any employee with access to the Trust intranet – this is restricted to input only and no other data can be accessed	

	Access to data is restricted to staff according to their role **User Permissions** DatixCloudIQ uses an Access Control list (ACL) framework to provision role-based access to the application and determine which users are granted access to which module records, as well as what operations they can perform on these records. The ACL framework supports both rule-driven and record-driven access to the application on the module-per-module basis. Permissions to create module records reside outside of record access rules and are provisioned as configuration settings. These settings are granular and can be applied at three levels: user level, user group level, and system (module) level. DatixCloudIQ user roles are divided into two major categories: administrator and non-administrator. The overall scope of an administrator role is to configure the system to meet business requirements, to administer users, and to manage the ACL framework. Non-administrator user roles refer to roles assigned to users to access module data in the application. Each module has a specific role set, and each role has specific permissions attached to it. For example, the Investigations module in the Evaluation toolkit includes the following roles: Investigation Lead, Investigator, Investigation Approver, Investigation Read Only, Investigation Deny. Administrator roles can be assigned at the user level, user group level, and system (module) level using configuration settings. Once the settings are applied, the corresponding users will get the administrator access to the specific are of the application. Non-administrative access is gained using rules and record level access (including record create permissions using the configuration settings).
2.5.2	Please provide a copy of the contract in place
	Datix Contract 2021.pdf
2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?
	Yes.

2.5.4	Is the supplier registered with the ICO? Please check the register	Yes	No
		Z8100369	
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	29.03.2021	Standards Met

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	Yes, however a certificate has not been provided	
	ISO 15489 Records Management		No
	ISO 27001 Information Security Standards	Yes ISO27001 2013 Certificate Datix.pdf	
	ISO 9001 Quality Management Systems	Yes	

2.5.10	Is the data held outside of the UK ie Europe, USA, Ireland? If yes please include the country		
	Yes	No	
		✓	
	If yes we need to seek assurance that the data will continue to flow post Brexit 31.12.2020, provide further detail below from the supplier		
	Not applicable		
2.6	Will this information be shared outside the organisations listed above?		
	Y/N	if answered **Yes** please describe organisation/s and geographic location	
	N		
2.7	Does the work involve employing contractors external to the Organisation?		
	Y/N	If **Yes**, provide a copy of the confidentiality agreement or contract?	
	Y	RLDatix consultant to assist with the implementation of the new software This is stated within the contract. Datix Contract 2021.pdf	
2.8	Has a data flow mapping exercise been undertaken?		
	Y/N	If **Yes**, please provide a copy here. If No, please explain why - YES	
	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	Information Flow Map Risk Managemei	
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	System access controls managed by the Risk Management team – all data changes are user and date stamped

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	Potential for an interface with CareFlow EPR. Mortality data outputs from CareFlow EPR auto uploaded to DatixCloudIQ. No DatixCloudIQ outputs will be fed into CareFlow EPR.

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?
	Incidents: all reviewed by GSU as part of the investigation process Risks: data reviewed periodically by risk owners/administrators and the Risk & Assurance Manager Legal and Patient Experience: data maintained by department staff Data will be deleted according to the Retention & Destruction Policy, although most information is currently kept in line with Goddard Inquiry
2.13	Who will have access to the information? (list individuals or staff groups)
	Risk Management team RLDatix Trust staff according to their role **IDENTITY & ACCESS MANAGEMENT** DatixCloudIQ supports the use of SAML 2.0-based identity providers, such as Microsoft's Active Directory Federation Services (ADFS) or CyberArk (previously Centrify/Idaptive) to manage user authentication. Integrating DatixCloudIQ with an identity provider ensures that no user

credentials are stored within the DatixCloudIQ platform, and, if linked to an existing domain, that users do not need to remember an additional set of credentials. Where supported by the chosen identity provider, this will allow the use of Multi-Factor Authentication (MFA), as well as Single Sign-On (SSO).

User Provisioning

User accounts are provisioned in DatixCloudIQ through an integration between customers' existing identity infrastructures, such as Active Directory (AD) and CyberArk. This integration is quick and requires a simple installation of the CyberArk Cloud Connector, which will be unique for each DatixCloudIQ customer. As many connectors can be installed as necessary (for example, for load balancing purposes) on any domain-joined machine. There is no need to open ports in customer firewalls, and there is no need for any dedicated hardware or additional infrastructure in customer DMZ.

User Authentication

When a DatixCloudIQ user accesses the application URL, DatixCloudIQ redirects the user's browser to CyberArk to authenticate. The authentication profile is configured to match with each customer's existing security policies. The authentication process is SAML-based and uses signed digital certificates and Public Key Infrastructure (PKI) to exchange security and identity related information between DatixCloudIQ and CyberArk. Upon successful authentication, the user is redirected back to the application URL.

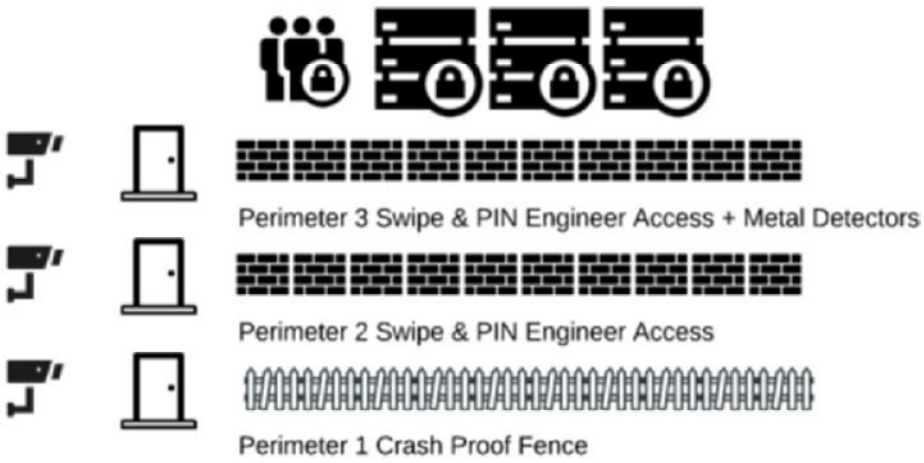
User Permissions

DatixCloudIQ uses an Access Control list (ACL) framework to provision role-based access to the application and determine which users are granted access to which module records, as well as what operations they can perform on these records. The ACL framework supports both rule-driven and record-driven access to the application on the module-per-module basis. Permissions to create module records reside outside of record access rules and are provisioned as configuration settings.

These settings are granular and can be applied at three levels: user level, user group level, and system (module) level.

DatixCloudIQ user roles are divided into two major categories: administrator and non-administrator. The overall scope of an administrator role is to configure the system to meet business requirements, to administer users, and to manage the ACL framework.

	Non-administrator user roles refer to roles assigned to users to access module data in the application. Each module has a specific role set, and each role has specific permissions attached to it. For example, the Investigations module in the Evaluation toolkit includes the following roles: Investigation Lead, Investigator, Investigation Approver, Investigation Read Only, Investigation Deny. Administrator roles can be assigned at the user level, user group level, and system (module) level using configuration settings. Once the settings are applied, the corresponding users will get the administrator access to the specific are of the application. Non-administrative access is gained using rules and record level access (including record create permissions using the configuration settings).	
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)	☐
	Logical Access Access to the DatixCloudIQ Production Network is granted through an established access control process restricted exclusively to RLDatix Operational Engineers. The principle of least privilege ensures that administrative users of the system only have the minimum rights necessary to perform their role. **Architecture**	

	The DatixCloudIQ architecture isolates infrastructure components by function and protects them in security zones. Each security zone has its own access control and monitoring with self-healing and service resumption capabilities. Single Point of Failure (SPOF) analysis and infrastructure reviews maintain a resilient system design.
2.14.2	What physical security measures have been implemented to secure access? ie swipe cards, digilock
	DatixCloudIQ data centres employ countermeasures to protect information assets using layered physical perimeter security, which includes 24/7 manned security, CCTV surveillance, swipe and pin access control, physical locks, and security breach alarms. Data centre equipment is controlled via a maintenance and inventory system with a certified destruction process that applies to servers and disk storage devices. DatixCloudIQ data centres use three layers of physical security on site. All three perimeters (Figure 1) must be traversed before access to the data halls is granted. Figure 1: Data Centre Perimeter Security  □ Perimeter 1: A crash rated penetration proof fence. □ Perimeter 2: Cooling, switchboards, and generators are blocked by solid walls. Entrances are restricted to service engineers requiring badge swipe and access pin. □ Perimeter 3: Entrances to the data halls, servers, and networking are monitored by CCTV and metal detectors and require another badge swipe and access pin for entry.
2.15	Will the data be stored on Trust servers
	Yes / No

		✓		
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	☐

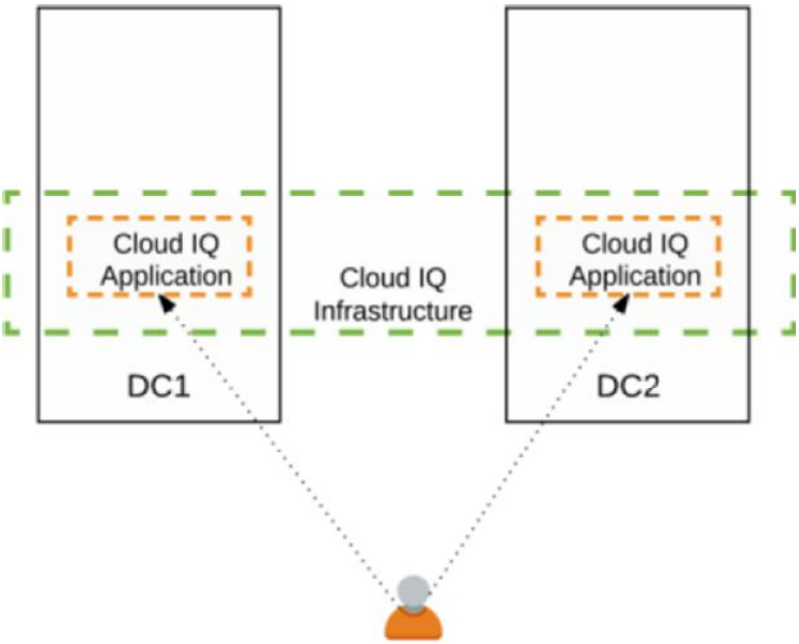
2.17	Are disaster recovery and business contingency plans in place for the information? What types of backups are undertaken i.e. full, differential or incremental?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The DatixCloudIQ infrastructure is designed and configured for redundancy and resilience with failover automation ensuring that data is always accessible and available. Business continuity is maintained with services remaining operational, accessible, and ready for use even during serious technical incidents. DatixCloudIQ leverages Amazon Web Services for its fully managed, policy-based backup solution. It is a continuous, automated backup process, retained for 30 days. All database backups are encrypted and stored such that only authorised personnel can access or restore data.

Data Centre & Service Availability

DatixCloudIQ is hosted across Tier IV mirrored data centres. Fully redundant in terms of circuitry, cooling, and networking, they provide an exceptionally high level of availability.

Should a single data centre or system become unavailable, the infrastructure will automatically redistribute servers and services across data centres in order to maintain availability.

Figure 2 illustrates the highly available and resilient DatixCloudIQ infrastructure mirrored across two data centres.



Disaster Recovery

DatixCloudIQ uses a tested disaster recovery (DR) plan and ensures services remain available or recoverable in case of disaster or the loss of a data centre. Full backups are taken daily with a thirty-day retention window and mirrored across all UK data centres.

Sensitive data is protected with AES-256 encryption with versioning and can be rolled back incrementally to earlier versions in an emergency.

RLDatix regularly simulates and tests infrastructure outages and analyses the latest threat vectors in order to

			ensure the stability and security of the DatixCloudIQ offering. The Trust maintains our own data so extraction can be performed at any time for use in our backup policies. The Trust is responsible for proper configuration and taking appropriate action to secure, protect and backup accounts and content in a manner that will provide appropriate security and protection. In the Trust we have a business continuity plan if the service was unavailable. The department would default back to paper records temporarily if required, for input to DatixCloudIQ at a later date. RLDatix have a full back-up server system so this should not be required for any length of time.
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	Staff are required to undertake annual mandatory Data Security training.	
2.19	Will reports be produced?		
	Will reports contain personal/sensitive personal or business confidential information?	Y	
	Who will be able to run reports?	System users (according to role/access) and system generated reports (scheduled)	
	Who will receive the reports and will they be published?	As required according to role	
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	Offboarding process included on page 8 of the contract
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?
		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. Legal purposes for SARS & legal, Police requests.
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.**
	Y	Once the data is inputted it remains as part of the audit trail but can be removed by a Datix Administrator if required
2.24	How much control will they have? Would they expect you to use their data in this way?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	N	Most data subjects would not be aware that their data is used for investigation purposes

<table>
<tr><td rowspan="4">2.25</td><td colspan="2">Are arrangements in place for recognising and responding to requests for access to personal data?</td></tr>
<tr><td>Y/N</td><td>Please describe if answered Yes. Please state why not if response is No.</td></tr>
<tr><td>Y</td><td>Ad-hoc reporting is available

Process in place to refer to IG or line manager if requester does not have access to specific records.

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)</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td rowspan="3">2.26</td><td colspan="2">Who are the Information Asset Owner(s) and Administrator(s)?</td></tr>
<tr><td>IAO</td><td>Shirley Higginbotham</td></tr>
<tr><td>IAA</td><td>Angela Farrands</td></tr>
<tr><td></td><td>System Administrators</td><td>Angela Farrands
Joanne Young
Neil Wilkinson
RLDatix</td></tr>
<tr><td rowspan="2">2.27</td><td colspan="2">How is the data secured in transit and at rest? Eg encryption, port control number</td></tr>
<tr><td colspan="2">CRYPTOGRAPHY

DatixCloudIQ encrypts and protects information that is stored (data at rest) and transmitted from the customer network to the DatixCloudIQ network (data in transit) using asymmetrical cryptography, this uses a private and a public key to protect both types of data and ensures that protected healthcare information can only be read by authorised users.

Encryption at Rest

DatixCloudIQ prevents sensitive data from being read by un-authorised users or applications with Server-Side Encryption (SSE) using the 256-bit Advanced Encryption Standard (AES-256). Data at rest cannot be viewed without a corresponding private key.</td></tr>
</table>

	Encryption at Transit DatixCloudIQ negotiates with customer systems when they connect to the DatixCloudIQ network using Transport Layer Security (TLS 1.2). This uses the Secure Hash Algorithm (SHA-256) for encryption and is the industry-standard for SSL certificates supported by current browsers providing authentication, privacy, and integrity. DatixCloudIQ administrative connections take advantage of RSA-based 4096-bit encryption. This combination of TLS, SHA-256, and RSA 4096-bit ensures all access to DatixCloudIQ is secure.	
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.**
	Y	DatixCloudIQ API integrations enable information in a customer's back-office healthcare systems to be shared with DatixCloudIQ without the need to replace existing applications. Standard integrations may involve copying of data from one system to another (data seeding) or may require continuous copying or synchronisation between DatixCloudIQ and the target application. RLDatix supports both standard and more complex bespoke integrations. Standard Integrations: DatixCloudIQ application modules contain integration interfaces that enable data sharing between DatixCloudIQ and healthcare computer systems such as contacts, medications, and personnel management using standards-based APIs.
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?
	Installation of the latest version of Datix would allow improved functionality, analytics and incident reporting, particularly relating to mortality reviews and Structured Judgement Reviews.
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?
	System users will be communicated with about the changes and to provide training. This document was presented to the Information Governance working group for consultation. Mortality module stakeholders to be asked to provide details of system parameters, required fields, etc. All module stakeholders to be part of the development and implementation process.

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).
	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
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)
	N/A – this is already provided for in the Patient Privacy Notice. This DPIA will be published once finalised.

2.34	What measures do you take to ensure processors comply?
	Incidents: all reviewed by GSU as part of the investigation process Risks: data reviewed periodically by risk owners/administrators and the Risk & Assurance Manager Legal and Patient Experience: data maintained by department staff. Datix is not aware of any sub processors involved in this project, for which it is responsible for ensuring compliance The Trust and RLDatix 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
	The Datix system and data would be held on a server managed and maintained by the system supplier, RLDatix, ensuring that system fixes and upgrades are performed promptly. A report to SIRO will be completed annually to provide assurance. Each time new functionality is added the DPIA will be reviewed. RLDatix will only ever process the Trust's data as per explicit agreement with the Trust. The Trust and RLDatix 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 RLDatix that is agreed to. The Service Agreement provides explicit information on processing activity provided by RLDatix as part of offering the service. There is limited scope to utilise the platform for other functions within the Trust. 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: Neil Wilkinson	Role: Risk and Assurance Manager	Date completed: 07/04/2021

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		2	2	**4**	
Loss of system data	Full system back-up process in place	3	2	6		3	2	**6**	
Leavers' access not removed	Datix system team notified of leavers by HR monthly Changes to user roles reviewed monthly via a Trust e-form report	3	1	3		3	1	**3**	
Business continuity plans in each area, do these exist and is there a template for recording if Datix goes down. Do you have an RPO or RTO	Business Continuity plan for the Datix system is in place Users of each module have business continuity plans for their areas/departments	3	1	3		3	1	**3**	

Risk Scoring Matrix.pdf

Stage – 4 Legal Compliance

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

Data Protection Act 2018	Compliance and Comment
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.