Healthier Communities, Outstanding Care

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

Data Protection Impact Assessment

Title	Ref number
QuitManager	

Introduction

A Data Protection Impact Assessment enables Sherwood Forest Hospitals NHS Foundation Trust (SFHFT) to meet its legal/compliance obligations with the Data Protection Act 2018 and the General Data Protection Regulation 2016.

The Data Protection Impact Assessment (DPIA) ensures the confidentiality, integrity and availability of information by applying a risk management process and gives confidence to interested parties that risks are adequately managed, as required under ISO/IEC: 27001:2017. It is important that the DPIA is part of and integrated with the organisation's processes and overall management structure and that information security is considered in the design of processes, information systems, and controls. The process identifies and allows issues to be mitigated at an early stage of implementation/change thereby reducing associated costs and damage to reputation. Data Protection Impact Assessment are an integral part of the "privacy by design" approach as identified by the Information Commissioner's Office.

Document Completion

A DPIA must be completed wherever there is **a change to an existing process or service** or **if a new process or information asset is introduced** that is likely to involve a new use or significantly changes the way in which personal data, special categories of personal data or business critical information is processed.

This document, and the privacy risks, actions and recommendations identified within it, will be accepted in the Project Sign Off (page 3). The project will need to signed off by the Information Asset Owner, Information Governance/Data Protection Officer and a customer representative (if applicable) and through the appropriate governance structure of the implementing organisation. Sign off and acceptance of the document does not close the privacy risks related to this project. It is important that the risks are revisited during the life of the project and any additional privacy risks identified are appropriately reviewed and mitigated.

PLEASE NOTE:

The Information Asset Owner (implementer) undertaking the Data Protection Impact Assessment has a responsibility to ensure that Patient Safety, Technical Security and Quality Impact Assessments are considered, in line with the Trust procedures.

Assessment Process Stages

Activity	IAO	Governance
Complete Title Bar and include Ref Number	x	
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:	**Bionical, QuitManager**. Installation of service and data management system

Project Description: Describe in sufficient detail for the proposal to be understood
QuitManager is a web based service database and management system for the use of the Tobacco Dependency Treatment Services for the inpatient and maternity team at Sherwood Forest Hospitals NHS Foundation Trust. It is required for the implementation of the NHS Long Term Plan Tobacco dependency programme.

Overview of the proposal: What the project aims to achieve
ICB funded installation of Bionical QuitManager, a patient database and service management system for the NHS Long Term Plan (LTP), in-house tobacco dependency treatment service; inpatient and maternity. Web based software. Stop smoking service industry standard product. Quit Manager - Bionical Maternity is an early implementer site for the NHS Long Term Plan (LTP) in house tobacco dependency treatment service. Commenced maternity pathway 5.12.21 and have waited for ICB funding until recently for a secure, interactive IT system to record patient activity and service management tool. NHS E and NHS I expected service programme for all maternity units from April 2022.

Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in DPIA assessment (name and job title):	Claire Allison, Tobacco dependence Maternity Lead

Project Sign Off

	Name	Job Title	Organisation	Date

Information Asset Owner	Lorraine Binch	Divisional General Manager	Sherwood Forest Hospitals NHS Foundation Trust	**21st December 2022**
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	**17th January 2023**
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	**21st December 2022**
Senior Information Risk Owner	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	**17th January 2023**
Caldicott Guardian	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	**28th November 2023**
Chief Digital Information Officer	Richard Walker	Chief Digital Information Officer	Sherwood Forest Hospitals NHS Foundation Trust	**28th November 2023**

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. Data is accessed inappropriately – individual username and passwords are provided.

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	**Recommendation Owner:**	**Agreed Deadline for action:**
Information Asset Administrators to ensure QuitManager is added to the information asset register and data flows are mapped and recorded	IAA	31st December 2022
Ensure business continuity plans are in place	IAA	31st December 2022
Account management Standard Operating Procedure generated and implemented, routine audit to take place	IAA	3 months post go-live

Stage 1 – Initial Screening Questions

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

Q	Screening question	Y/N	Justification for response
1	Will the project involve processing of information about individuals	Y	Tobacco dependence treatment service activity in maternity and for inpatients. Mandatory national reporting requirement
2	Will the project compel individuals to provide information about themselves?	Y	Information already provided to maternity and inpatient service
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Y	Bionical host the virtual QuitManager software programme. NHS Digital receive patient level data and then NHS Digital anonymise the information in order to populate a national database for reporting tobacco outcomes in line with the NHS Long Term Plan.
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	The data collected is only relevant to the service being provided by the inpatient and maternity tobacco dependence treatment services. The service team will keep personal information up to date at each contact.
6	Are there security arrangements in place while the information is held?	Y	Bionical host the virtual QuitManager software programme and the programme will require log in and password security.

Q	Screening question	Y/N	Justification for response
7	Does the project involve using new technology being introduced?	Y	Web based information management system
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	
9	Does the project include any of the following activities? (Mark all that apply and a description if answered 'Y')		
9.1	Evaluation or scoring - including profiling, predicting and transactional monitoring techniques. For example, a biotechnology company offering genetic tests directly to consumers in order to assess and predict the disease/health risks; a new system that might be susceptible to fraud or abuse, and if so whether it ensures that the system has the capability for transactional level monitoring so you can audit the transactions if needed as part of an investigation.	N	
9.2	Automated decision making with legal or similar significant effect - processing that aims at taking decisions on individuals without human intervention. For example, the processing may lead to the exclusion or discrimination against individuals.	N	
9.3	Systematic monitoring of individuals* (e.g. CCTV, body camera's, health data through wearable devices) processing used to observe, monitor or control individuals. For example, monitoring of the employees' work station, internet activity, etc.	N	
9.4	Matching or combining datasets - for example originating from two or more data processing operations performed for different purposes and/or by different data controllers in a way that would exceed the	Y	The single monthly NHS Digital patient level data report is collated from the current separate maternity and inpatient tobacco service database (that will be QM in the future).

Q	Screening question	Y/N	Justification for response
	reasonable expectations of the data subject		
9.5	Data concerning vulnerable individuals - individuals may be unable to easily consent to, or oppose, the processing of their data, or exercise their rights. Vulnerable individuals may include children, employees, more vulnerable segments of the population requiring special protection (mentally ill persons, asylum seekers, or the elderly, patients, etc.).	N	
9.6	Innovative use or applying new technological or organisational solutions - combining the use of finger print and face recognition for improved physical access control. Implementation of a new technology, system or business process or collection of new information	N	
9.7	Offer online services directly to children	N	
9.8	Storing or transferring data outside the EU (e.g. cloud computing, accessing data outside the EU, use of an American transcribe company)	N	
9.9	Direct marketing (e.g. newsletters, postcards, telemarking, e-mail subscriptions)	N	
If you have answered “Yes” to any of the questions numbered 1-9 please proceed and complete stage 2.			
10	Is a Patient Safety Review required? [DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital]()	N	18.10.2022 – this is a patient administration service only. Clinical information will be recorded on BadgerNet
11	Is a Quality Impact/Technical Security Review required?	Y	15.12.2022 - NHIS have reviewed the supplier assurance framework and have not identified any

Q	Screening question	Y/N	Justification for response
			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)		Ethnicity code			
	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)		Tobacco use			

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					
	Data will be sent using HL7. SSL (Security Socket Layer) and HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) are used in the encrypted transmission of data.					

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	Patient database and service management system. To facilitate patient journey through tobacco quit programme and mandatory national and local data reporting
2.3.1	How will you collect, use, store and delete data?	
	Referral from inpatient (Nervecentre) and maternity service (ORION or BadgerNet to nhs.net acc). Data input by tobacco dependence treatment service staff in maternity and inpatients. The data will be used for patient treatment management, plus local and national mandatory reporting. 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)	
	Service users and referrals from in-house employees or out of area midwives.	
2.3.3	How much data will you be collecting and using?	
	Approximately 600 individuals per year from maternity service Approximately 400 individuals per year from in-patient service	
2.3.4	How often? (for example, monthly, weekly)	
	Daily from referrals from inpatient and maternity sources.	

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
	The right to erasure - Not applicable in this circumstance as the data is being processed under UK GDPR Article 9(2)(h) the processing is necessary for the purposes of preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services. This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (e.g. a health professional). The right to data portability - Not applicable in this circumstance as the legal bases for processing the data are neither consent nor for the performance of a contract.
2.3.6	Where will the data be stored? i.e., CareFlow, Shared Drive, offsite storage
	QuitManager is hosted by Bionical. All data is held within the Bionical QuitManager web based application. All data is held within the UK. biconical use Rackspace for all hosting and Redcentric for offsite backups **Rackspace Hosting Environment** Bionical have used Rackspace managed hosting of their dedicated servers for hosting solutions since 2008. Data is located in the Slough datacentre in the UK. Rackspace Ltd, Hyde Park Hayes, 5 Millington Road, Hayes, Middlesex, UB3 4AZ, Tel: 0800 988 0300 https://www.rackspace.com/en-gb **Redcentric off-site backup provider** Bionical have used Redcentric for their off-site backups since 2011. All data is held in the Harrogate data centre in the UK. Central House Beckwith Knowle, Harrogate, HG3 1UG Tel: 01423 850000 http://www.redcentricplc.com/about-us/our-uk-data-centres/harrogate-data-centre/
2.3.7	How many individuals are affected?
	The number of affected individuals is around Approximately 600 individuals per year from maternity service and approximately 400 individuals per year from in-patient service.

2.3.8	What geographical area does it cover?
	Service users at the Trust from Mansfield, Ashfield, Newark, Sherwood and other areas of Nottinghamshire. Plus out of Nottinghamshire eg Derbyshire, Lincolnshire and surrounding counties.

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
	Bionical	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** Supplier Assurance Framework TEMPLATI Supplier Assurance Framework - Example Cloud Assessment.xlsx
	Y	NHIS have reviewed the attachments and assessed as low risk. Supplier Assurance Framework TEMPLATE
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

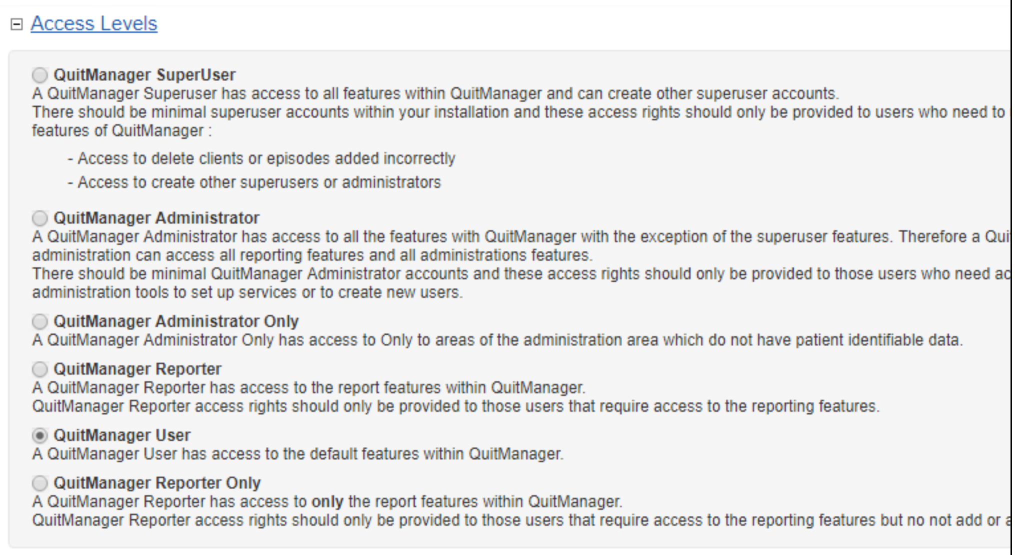
Account
Management & Acces

Each user needs a username and password to access data. The password strength is high. The Trust will have administrators within the team who will invite others to join and be able to monitor their access.

By default, the system has multiple roles available, namely:

- Super User
- Administrator
- User
- Reporter
- Advisor

Example of setting roles within QuitManager:



⊟ Access Levels

○ **QuitManager SuperUser**
A QuitManager Superuser has access to all features within QuitManager and can create other superuser accounts.
There should be minimal superuser accounts within your installation and these access rights should only be provided to users who need to
features of QuitManager :

- Access to delete clients or episodes added incorrectly
- Access to create other superusers or administrators

○ **QuitManager Administrator**
A QuitManager Administrator has access to all the features with QuitManager with the exception of the superuser features. Therefore a Qui
administration can access all reporting features and all administrations features.
There should be minimal QuitManager Administrator accounts and these access rights should only be provided to those users who need ac
administration tools to set up services or to create new users.

○ **QuitManager Administrator Only**
A QuitManager Administrator Only has access to Only to areas of the administration area which do not have patient identifiable data.

○ **QuitManager Reporter**
A QuitManager Reporter has access to the report features within QuitManager.
QuitManager Reporter access rights should only be provided to those users that require access to the reporting features.

● **QuitManager User**
A QuitManager User has access to the default features within QuitManager.

○ **QuitManager Reporter Only**
A QuitManager Reporter has access to **only** the report features within QuitManager.
QuitManager Reporter access rights should only be provided to those users that require access to the reporting features but no not add or a

Within these roles additional permissions can be defined on an individual basis.

	QuitManager can be configured to restrict access to patient identifiable data, allowing for reporting on anonymised data at commissioner level. Template.docx			
2.5.2	Please provide a copy of the contract in place			
	SFH_HW_Q001 Sherwood Forest QM			
2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?			
	Bionical offer various options regarding data transfer for retention and processes for destruction at the expiration of the contract.			
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	Completed: Yes/No	Date submitted	Standard Met/Not Met
		Yes	21st June 2022	Standards Met

	following details			

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 Bionical Solutions - Cyber Essentials.pdf
	ISO 15489 Records Management		x
	ISO 27001 Information Security Standards	X ISO 27001_2013 Certificate - 04 Jan 20	
	ISO 9001 Quality Management Systems	X ISO 9001_2015 Certificate - 04 Jan 20	

2.5.10	Is the data held outside of the UK ie Europe, USA, Ireland? If yes please include the country	
	Yes	No
		x
	If yes we need to seek assurance that the data will continue to flow post Brexit 31.12.2020, provide further detail below from the supplier	

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?				
	N					
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					
	The Trust will need to map the flow of data for this service. Added as a recommendation.					
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?				
		QuitManager has comprehensive auditing built in. This ensures we can easily track who is making changes to records. This includes Login ID and Timestamps All system access and changes to data are audited. This data can be retained indefinitely or for a requested timescale. Should a rogue user maliciously damage data, the above process would allow us to recover the data and the audit tools would allow us to identify who was involved. This has been used on a number of occasions to support NHS Fraud investigations.				
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	Potential in the future for QuitManager to link with the maternity database BadgerNet.				

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 right to rectification - People can inform us if they think we hold inaccurate information about them. These requests will be considered on a case-by-case basis. Tobacco dependence treatment team staff to maintain information for accuracy and change appropriately.	
2.13	Who will have access to the information? (list individuals or staff groups)	
	Tobacco dependence treatment service team for maternity and inpatients.	
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)	☐
	Access to QuitManager is granted through an established access control process restricted exclusively to Bionical Operational Engineers. The principle of least privilege ensures that administrative users of the system only have the minimum rights necessary to perform their role.	

2.14.2	What physical security measures have been implemented to secure access? ie swipe cards, digilock			
	The following security measures are in place (Bionical) to prevent data loss or breach: • **No public access** – Rackspace own and manage all of their equipment. This means the only people who have access to the physical equipment are the Rackspace engineers. • **Video Surveillance** – 24 hour monitoring of all data facilities is in place. This includes all entrances/exits and the data centre itself. • **Onsite security personnel** – onsite security personnel monitor each data centre building 24 hours a day, 7 days a week. This is the first layer of security. • **Biometric Security** – Hand scanners are used as the second layer of security for access to the data centre. • **Pass cards** – work in conjunction with the hand scanners to ensure access is restricted to those with a pass card.			
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	☐
	SSL (Security Socket Layer) and HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) are used in the encrypted transmission of data. In order to ensure that data are accessed as expected, we have taken the following measures:			

	1. A firewall is used to filter malicious access. 2. Intrusion detection is used to detect system anomalies. 3. Malicious Code Protection is used to perform security checks on all committed data.	
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	In the Trust 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. All data stored on the suppliers servers is backed up at hourly intervals. They can restore from any of these hourly snapshots from the previous 49 hours. Beyond that they can restore a daily backup for the previous 9 days. Weekly backups would be available beyond this point. **biconical use Rackspace** (www.rackspace.co.uk) to host data. Multiple levels of security are employed to ensure that the data we store here is safe. Should a total disaster wipe out the Rackspace datacentre, we have facilities within other data centres where we could rebuild the server environment. **biconical use Redcentric** (www.redcentricplc.com) to store weekly backups for disaster recovery purposes. The data is compressed and encrypted before being transferred to the Redcentric servers on a weekly basis. Redcentric are accredited to store HM Government “Restricted” data and are also compliant with the NHS Digital Information Governance Statement of Compliance (IGSoC). They are a trusted NHS Digital partner.
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	Trust staff are required to undertake annual mandatory IG training. Trust employees will receive training on how to use the QuitManager programme. Bionical to supply a training guide to support this 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?	TDTS service leads
	Who will receive the reports and will they be published?	SFHFT BI team to forward to NHS Digital, patient identifiable information. LMNS and ICB for Nottingham and Nottinghamshire require numerical data reports.
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 information contained in QuitManager will be replicated from BadgerNet.
2.21	Is consent required for processing of personal data?	
	Y/N	Please describe if answered **Yes**
	N	Existing NHS data legislation regulations
		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?

		UK GDPR Article 6(1)(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract UK GDPR Article 6(1)(c) processing is necessary for compliance with a legal obligation to which the controller is subject UK GDPR 6(1)(e) public interest or public duty UK GDPR 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 right to be informed - Transparency information and materials will be available to people when they are admitted to the ward. This information will also be available on all participating organisations' websites. The Trust's privacy notice is here https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/ Supplier privacy notice Privacy Policy - biconical The right to object - People can object to their information being used for any purpose, and these objections will be considered on a case-by-case basis.
2.23	Is there a process in place to remove personal data if data subject refuses/removes consent	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**

	N	Part of our statutory duties under UK GDPR Article 6(1)(e) public interest or public duty, and UK GDPR 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. The right to restrict processing - People can request the use of their data to be restricted in certain circumstances. These will be considered on a case-by-case basis. The right to data portability - Not applicable in this circumstance as the legal bases for processing the data are neither consent nor for the performance of a contract. The right to object - People can object to their information being used for any purpose, and these objections will be considered on a case-by-case basis.
2.24	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	The data collected will form the basis of their personal care pathway and enable communication between health care practitioners.
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	Phil Bolton
	IAA	Claire Allison
	System Administrators	Claire Allison, Tanya Noble-Jepson, Lisa Hardy, Amy Bower, Ian Ferris, Donnah Taylor, Su Barnfather
2.27	How is the data secured in transit and at rest? Eg encryption, port control number	
	The solution is web based and secured by SSL using SHA 256 – Key Strength 2048 bits The interface is only exposed for Web traffic (ports 80 and 443) and firewalls are in place to deny traffic on any other ports.	
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]
		A patient safety case is not required. Supplier assurance framework has been reviewed by NHIS. No risks or recommendations identified.
2.29	Are there any current issues of public concern that you should factor in?	
	Y/N	Please describe if answered **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 management of patients who are receiving treatment from the tobacco dependency treatment services at SFHFT.	
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?
	Claire Allison, Tobacco Dependence Maternity Lead 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).
	The Trust's lawful basis for processing personal and special categories of personal data are:

	1. UK GDPR 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. UK GDPR 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. UK GDPR 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. UK GDPR 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. UK GDPR 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.

2.34	What measures do you take to ensure processors comply?
	Bionical is not aware of any sub processors involved in this project, for which it is responsible for ensuring compliance. The Trust and Bionical 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

	Bionical will only ever process the Trust’s data as per explicit agreement with the Trust The Trust and Bionical have a contract in place where roles and responsibilities are defined. 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: 20th October 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 due to connection failure or server failure either via NHIS or 3rd party supplier. This could result in the service being disrupted or unavailable. The consequences of this could be financial penalties and reputational damage to the Trust	Full system back-up processes and ISO 27001 accreditation in place Business continuity plan in place Regular updates from supplier to advise users of any planned updates and a process is in place to contact all main users for support during any unplanned downtime	2	2	4		2	2	4	Manual input, business continuity plan to be used

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 data due to connection failure or server failure by third party supplier. This could result in the service being disrupted or unavailable. The consequences of this could be financial penalties and reputational damage to the Trust	Full system back-up processes and ISO 27001 accreditation in place Business continuity plan in place	2	2	4		2	2	4	Manual input, business continuity plan to be used
Data is accessed inappropriately due to lack of access controls. Movers and leavers access not removed. Data is inappropriately	Username and password controls in place. Access is managed within the team. Account Management and access procedure to be audited on a regular basis. Appropriate access according to role. IG Training in place.	2	2	4		2	2	**4**	Routine audits. Information governance training up to date

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)**	
processed and/or disclosed				🟩				🟩	

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.