Healthier Communities, Outstanding Care

NHS
Sherwood Forest Hospitals
NHS Foundation Trust

Data Protection Impact Assessment

Title	Ref number
MedICUs HEART FAILURE DATABASE	

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:	**Implementation of MedICUs Heart Failure**

Project Description: Describe in sufficient detail for the proposal to be understood
Implementation of MedICUs Heart Failure, a NICOR Heart Failure conforming data-base system to facilitate the service's audit compliance with the national mandatory minimum data set in a time efficient manner. In addition to conforming to national mandatory requirements, the system facilitates localised service audits to help perceive the underlying fundamentals that define the service for the benefit of service and individual patient level analytics.

Overview of the proposal: What the project aims to achieve
The project aims to return time to nursing by streamlining the NICOR Heart Failure conforming process as well as facilitate efficient auditing (compliant with national data opt-outs) for the benefit of identifying where the service can implement change for the benefit of patient outcomes.

Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in DPIA assessment (Include Email Address):	Sarah Doughty, Assistant General Manager Gail Moore, Heart Failure Specialist Nurse Alison Beal, Heart Failure Specialist Nurse

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Lizzie Beaumont	Interim Divisional General Manager	Sherwood Forest Hospitals NHS Foundation Trust	7th October 2022

Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	4th May 2022
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	19th April 2022
Senior Information Risk Owner	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	6th October 2022
Caldicott Guardian	Dr David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	21st September 2022
Chief Digital Information Officer	Richard Walker	Chief Digital Information Officer	Sherwood Forest Hospitals NHS Foundation Trust	21st September 2022

Assessment Summary

To be completed by Information Governance

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

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks:

Summary:

Legislative Compliance:

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.

UK GDPR 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)

UK GDPR 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, Information Asset Management and patient safety.

Risks

1. Loss of system access/data - Full system back-up process in place
2. MedICUs will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO
3. Data is accessed inappropriately – individual username and passwords are provided.

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations: Information Asset Administrators to ensure MedICUs is added to the information asset register and data flows are mapped and recorded User access and permissions SOP to be reviewed to ensure appropriate for system access	**Recommendation Owner:** IAA	**Agreed Deadline for action:** 28th October 2022

Stage 1 – Initial Screening Questions

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

Q	Screening question	Y/N	Justification for response
1	Will the project involve the collection of information about individuals?	Y	Collation of patient data for national audits (NICOR)
2	Will the project compel individuals to provide information about themselves?	N	Not above what is already collated for care pathway or existing audits
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	N	Database does allow CSV file upload to national NICOR audits. The service is following the Trust's national data opt-outs procedure and patients who have opted out will not be entered.
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	Interfaces to CareFlow EPR and ICE. MedICUs updates national minimum dataset for data collection
6	Are there security arrangements in place while the information is held?		
7	Does the project involve using new technology to the organisation?	Y	MedICUs web tool
8	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	N	
If you have answered "Yes" to any of the questions numbered 1-8 please proceed and complete stage 2.			

Q	Screening question	Y/N	Justification for response
9	Is a Patient Safety Review required? DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital	Y	6th June 2022 a patient safety case has been undertaken.
10	Is a Quality Impact/Technical Security Review required?	Y	3rd March 2022 - NHIS have reviewed the supplier assurance framework and have not identified any concerns or recommendations

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

Stage 2 – Data Protection Impact Assessment

2.1	What is the change					
	New purpose?	☐	Revised/changed?	☐	Other?	☒
	If Other please specify.		Upgrade from access database to web tool			

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)		NICOR minimum dataset (see data capture form) Copy of Heart Failure pro forma 20			
	Sensitive Personal Data (special categories):					
	Children					☐
	Vulnerable groups					☒
	Racial or ethnic origin					☒
	Political opinion					☐
	Religious Belief					☐
	Trade Union Membership					☐
	Physical or mental health or condition					☒
	Sexual Health					☐
	Criminal offence data					☐

	Other data (please specify)	

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

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	Collate national audit data and share patient data across the Acute nursing team for the purpose of managing the care pathway.

2.3.1	How will you collect, use, store and delete data?
	Data input at source from patient consultation both face to face and virtual/phone. Stored within the MedICUs web platform, on Trust servers on site
2.3.2	What is the source of the data? (i.e. from data subject, system or other third party)
	Data from patient consultation and patient record
2.3.3	How much data will you be collecting and using?
	See above minimum data set capture form. Circa 10,000 patient records.
2.3.4	How often? (for example, monthly, weekly)
	Capture of daily patient consultations
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
	MedICUs to store in line with code of practice timeframes.

2.3.6	Where will the data be stored? i.e., CareFlow, Shared Drive, offsite storage
	On a trust server.
2.3.7	How many individuals are affected?
	Circa 10,000 records
2.3.8	What geographical area does it cover?
	Heart failure patients accessing Sherwood Forest Hospitals service.

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
	MedICUs	Data Processor

2.5	If we have identified a supplier in 2.4, the following questions for 2.5 will need to be answered by the **supplier and the Trust**	
	Y/N	**If yes the third party will need to complete the following assessment. This will need to be provided in addition to the completion of this proforma. An example of a completed assessment is also provided below** NHIS - Supplier Assurance Framewo

		SAF - Medicus Heart Failure.xlsx		
2.5.1	Please describe access and controls in place Account access management Standard Operating Procedure to be completed prior to the implementation of the project https://www.sfh-tr.nhs.uk/media/12007/ig-012-account-management-and-access-policy-2021.pdf Account ManagementSOP Ten			
	Account Management & Acces			
2.5.2	Please provide a copy of the contract in place			
	PO.pdf MELA SOLUTIONS SOFTWARE LICENCE A			
2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?			
	Yes see section 12. MELA SOLUTIONS SOFTWARE LICENCE A			
2.5.4	Is the supplier registered with the ICO? Please check the register	Yes	No	
		Yes Registration number: Z8172745		
2.5.5	Has the supplier received ICO Enforcement? Please check the register	Yes	No	
			NO	

2.5.6	Has the supplier received ICO Decision Notice? Please check the register	Yes	No
			NO
2.5.7	Has the supplier received an ICO Audit? Please check the register	Yes	No
			No

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	30th June 2022	Standard 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		x
	ISO 15489 Records Management		x
	ISO 27001 Information Security Standards		x
	ISO 9001 Quality Management Systems		x

2.5.10	Is the data held outside of the UK ie Europe, USA, Ireland? If yes please include the country	
	Yes	No
		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	

<table>
<tr><td rowspan="3">2.6</td><td colspan="5">Will this information be shared outside the organisations listed above?</td></tr>
<tr><td>Y/N</td><td colspan="4">if answered Yes please describe organisation/s and geographic location</td></tr>
<tr><td>Yes</td><td colspan="4">NICOR, UK based definers of national minimum data-set, will receive audits from trust that have been consented by patients</td></tr>
<tr><td rowspan="3">2.7</td><td colspan="5">Does the work involve employing contractors external to the Organisation?</td></tr>
<tr><td>Y/N</td><td colspan="4">If Yes, provide a copy of the confidentiality agreement or contract?</td></tr>
<tr><td>Y</td><td colspan="4">MELA SOLUTIONS SOFTWARE LICENCE A</td></tr>
<tr><td rowspan="3">2.8</td><td colspan="5">Has a data flow mapping exercise been undertaken?</td></tr>
<tr><td>Y/N</td><td colspan="4">If Yes, please provide a copy here. If No, please explain why</td></tr>
<tr><td colspan="5">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</td></tr>
<tr><td>Y</td><td colspan="5">Copy of Cardiology Data Flow Map July 2(

The attached draft information flows will be updated once the new system is in place and the standard operating procedures have been developed.</td></tr>
<tr><td rowspan="2">2.9</td><td colspan="5">What format is the data?</td></tr>
<tr><td>Electronic</td><td>☒</td><td>Paper</td><td>☐</td><td>Other (Please describe)</td><td>Click here to enter text.</td></tr>
<tr><td rowspan="2">2.10</td><td colspan="5">Is there an ability to audit access to the information?</td></tr>
<tr><td>Y/N</td><td colspan="4">Please describe if answered Yes. If NO what contingencies are in place to prevent misuse?</td></tr>
</table>

	Y	Permissions preventing auditing, editing and viewing of records can be defined by the administrator for users with logins. SuperUsers can run reports on their data. SuperUsers are not currently able to query or interact with the audit table. There are plans to make this available but this is unlikely to happen until late 2022. The data is installed on a Trust server. Mela will have access for the purposes of providing a support service only.

2.11	Does the system involve new links with personal data held in other systems or have existing links been significantly changed?	
	Y/N	Please describe if answered **Yes**
	Y	The previous system did not integrate with CareFlow EPR and ICE, this new system will.

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?
	Demographics will be fed through by CareFlow EPR integration
2.13	Who will have access to the information? (list individuals or staff groups)
	Medical staff from the Heart Failure team. The Trust upload a weekly CSV file to the NICOR web portal

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)	☐

2.14.2	What physical security measures have been implemented to secure access? ie swipe cards, digilock			
	All access is role based. Admin / User rights. There are different levels for the password strength with a combination of characters from at least two groups (medium) and three groups (strong level) from the following groups: Upper-case letters, Lower-case letters, numbers, and non-alphanumeric symbols. Token generation is also used for new accounts			
2.15	Will the data be stored on Trust servers			
	Yes	No		
	x			
2.16	Please state by which method the information will be transferred?			
	Email (not NHS.net)	☐	NHS.net	☐
	Website Access (internet or intranet)	☒	Wireless Network (Wi-Fi)	☐
	Secure Courier	☐	Staff delivered by hand	☐
	Post (internal)	☐	Post (external)	☐
	Telephone	☐	SMS	☐
	Other	☐	please specify below	☒

	Data is encrypted using 256bit encryption. Mela require remote access to the Trust server hosting the MedICUs application via a trust approved VPN/ VDI solution.	
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.**
	Yes	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 in the case notes or access the Portal directly. The supplier has a Disaster recovery plan documented.
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	Included as part of the subscription to the system, training includes defining of appropriate user permissions
2.19	Will reports be produced?	
	Will reports contain personal/sensitive personal or business confidential information?	
	Who will be able to run reports?	Users with auditing permissions. SuperUsers can run reports on their data. SuperUsers are not currently able to query or interact with the audit table. There are plans to make this available on the user side but

		this is unlikely to happen until late 2022. The data is installed on a Trust server. Mela will have access for the purposes of providing a support service only.
	Who will receive the reports and will they be published?	NICOR

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 supplier uses a dedicated tool called Wipe File to securely remove data

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 UK GDPR 6(1)(e) public interest or public duty, and Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

2.22	Will individuals be informed about the proposed uses and share of their personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The Trust's privacy notice is here https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/ The National Heart Failure Audit collects data on patients with an unscheduled admission to hospital in England and Wales who are discharged with a primary diagnosis of heart failure. The audit aims to drive up the quality of the diagnosis, treatment and management of heart failure by collecting, analysing and disseminating data, and eventually to improve mortality and morbidity outcomes for heart failure patients. The audit is managed by NICOR, with clinical direction and strategy provided by the **British Society of Heart Failure (BSH)**. The audit is commissioned by the **Healthcare Quality Improvement Partnership (HQIP).** The National Heart Failure Audit was established in 2007. The audit aims to capture data on clinical indicators which have a proven link to improved outcomes for heart failure patients, and to encourage the increased use of clinically recommended diagnostic tools, disease modifying treatments and referral pathways. The dataset is updated periodically to ensure that the data collected remains in line with contemporary clinical guidance, and clinical input has been integral to the decision-making and running of the audit since its inception.
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	Records can be deleted from the system provided the user has administrator user rights
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	Direct healthcare
2.25	Are arrangements in place for recognising and responding to requests for access to personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
		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	Divisional General Manager – Medicine
	IAA	Gail Moore, Jenni Read and Julie Rhodes
	System Administrators	Gail Moore, Jenni Read and Julie Rhodes
2.27	How is the data secured in transit and at rest? Eg encryption, port control number	
	The data is transmitted via HL7 and encrypted both in transit and at rest. HL7 - Health Level Seven® International (HL7®) is the global authority on standards for interoperability of health technology and is the global industry standard for passing healthcare data between systems.	
2.28	Has the impact to other NHIS systems/processes been considered and appropriate SBU's consulted and in particular technical security?	
	Y/N	Please describe if answered **Yes.** Please state what checks were undertaken if response is answered **No.**
		The 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 with heart failure conditions.	
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?	
	Mela Solutions will support the Trust by providing the necessary feedback on MedICUs System technical and GDPR aspects. Gail Moore and Joanne Davies 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. The Trust's privacy notice has been updated.

2.34	What measures do you take to ensure processors comply?
	Mela Solutions is not aware of any sub processors involved in this project, for which it is responsible for ensuring compliance The Trust and Mela 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
	Mela will only ever process the Trust's data as per explicit agreement with the Trust. The Trust and Mela 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 Mela that is agreed to. The Service Agreement provides explicit information on processing activity provided by Mela as part of offering the MedICUs System service. Mela is set up with the view to provide health care professionals within the Trust information on patients using MedICUs. As such, 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	Gina Robinson	Role:	Information Security Officer	Date completed: 25th March 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)**	
If the system is not recorded on the information asset register, the Trust would not have a record of the data flows	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 via the patient's case notes	2	2	4	MedICUs will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO	2	1	**2**	MedICUs will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO
Loss of system access/data 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 patient harm, financial penalties and reputational damage to the Trust	Full system back-up process in place	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)**	
Data is accessed inappropriately due to lack of access controls. Movers and leavers access not removed. Data is inappropriately processed and/or disclosed	Username and password controls in place. Account Management and access procedure in place. Appropriate access according to role.	2	2	4	Access data inappropriately	2	1	**2**	Ensure access is managed and leavers list is received and actioned. Routine audits.

Risk Scoring Matrix.pdf

Stage – 4 Legal Compliance

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

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

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

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