

Data Protection Impact Assessment

Contents

Introduction	2
When and who should complete a DPIA?	2
Who do I send the completed DPIA to for review?	2
What if I need help?	2
Step 1 – What is the aim of the project being undertaken	3
Step 2: What type of data is being processed?	10
Step 3 – Data security	17
Step 4 – Data use and sharing	22
Step 5 – Processing by or with a supplier/third party	24
Step 6 – Consultation	25
Step 7 – Lawful basis	26
Stage 8 – Risk Template	28
Step 8 – Legal compliance	34
Step 9 - Assessment Summary	38
Step 10 - Recommendations for Action	40
Step 11 - Project signoff	41

Introduction

Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the UK General Data Protection Regulation's fundamental principles and requirements, and forms part of the focus on accountability.

A Data Protection Impact Assessment (DPIA) is a tool that we use to identify and reduce the data protection risks of our processing activities. They can also help us to design more efficient and effective processes for handling personal data.

The UK General Data Protection Regulation requires the Trust to put in place appropriate technical and organisational measures to implement the data protection principles effectively and safeguard individual rights. This is 'data protection by design and by default'.

In essence, this means we have to integrate or 'bake in' data protection into our processing activities and business practices, from the design stage right through the lifecycle. This concept is not new and **is now a legal requirement**.

When and who should complete a DPIA?

- 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. **No commitments to, or installation of systems, should take place before the DPIA has been signed off.**
- Information Assets Owners (IAO) and Information Assets Administrators (IAA) **must** complete the DPIA.
- Relevant stakeholders (internal and external suppliers) should be consulted throughout the DPIA process.

Who do I send the completed DPIA to for review?

- Information Governance Team sfh-tr.information.governance@nhs.net.

What if I need help?

- Please contact the Information Governance Team sfh-tr.information.governance@nhs.net or [SFHT Phonebook \(nnotts.nhs.uk\)](http://SFHT.Phonebook(nnotts.nhs.uk))

IMPORTANT – PLEASE COMPLETE ALL QUESTIONS. IF YOU THINK A QUESTION DOES NOT APPLY INSERT N/A AND EXPLAIN WHY.

Project title:	Critical Care Unit - Medicus
Reference number:	
Implementing organisation:	Sherwood Forest Hospitals NHS Foundation Trust
Key contacts involved in the DPIA (name and job title)	Vishal Dhokia SFH Specialty Head of Service Arron Smith Assistant General Manager Karen Mellors NHIS Project & Business Change Manager
Information Asset Owner (name and job title)	Vishal Dhokia Specialty Head of Service
Information Asset Administrator (name and job title)	Sharon Fleming Administrator

Step 1 – What is the aim of the project being undertaken

Q1	Project description: Describe in sufficient detail for the project to be understood	<p>The Adult Critical Care Unit (ACCU) have a requirement for a specialised software system for the collection, auditing, reporting and submission of mandatory data for national benchmarking to the Intensive Care National Audit & Research Centre (ICNARC) and the Critical Care Minimum Dataset (CCMDS) to finance for commissioning purposes.</p> <p>Medicus will be used purely for national reporting purposes to submit data to ICNARC. The Department use other systems for clinical purposes e.g. Nervecentre.</p> <p>Mela Solutions Ltd provide the Medicus ICU software system which has been widely used across the NHS for the past 20+ years. Medicus ICU provides units with a stable and proven solution for the data collection and auditing of the latest ICNARC, CCMDS and HRGs datasets together with providing all of the tools</p>
-----------	--	--

		<p>required for their local auditing requirements. This software will be installed on a local hospital server with all associated data contained within. User access to the system is via web browser from any trust internet enabled device including PC, laptop or tablet.</p> <p>Additionally, the project includes the development of a HL7 ADT Integration between Medicus ICU and the existing hospital PAS/EPR system provided by System C. This link will automate patient demographic, hospital and unit admission and discharge information for each patient entered into the Medicus ICU system. Automation of this basic level of data proposes to save significant data entry time.</p>
--	--	--

<p>Q2</p>	<p>Why are we doing it?</p> <p>Summarise why there is a need for implementation or change and the benefits it will realise.</p>	<p>Mitigate risk: Submission to ICNARC national audit is a mandatory requirement as part of national service specification for Adult Critical Care units. The current contract with existing software supplier (Medtrack) will terminate on 31st March 2024 necessitating an alternative solution.</p> <p>Improved Efficiency:</p> <ul style="list-style-type: none"> • Medicus ICU is a digital solution, providing clinicians, managers and clerical staff with access to all of the information they require on PC's, laptops or tablets anywhere in the Trust. • Fully customisable beds dashboard, set up per critical care unit, with an overview of all activity (including safety alerts) for each patient, together with bed history and all pending booked patients. • Key performance indicator (KPI) dashboards provide clinicians with a vast range of data indicators at their fingertips. • Data duplication is reduced through integration with existing hospital
------------------	--	--

systems via HL7 ADT feeds to automate patient demographic, hospital and unit admission and discharge information. Data is shared between fields within Medicus ICU where possible to reduce duplication and streamline user experience.

Added Value:

- Key performance indicator (KPI) dashboards to summarise Trust level indicators such as mortality rates, sepsis & infections and adverse events amongst others are available to managers and consultants alike to improve the visibility of key data for critical care teams, removing the dependence on paper records.
- Patient interventional data recorded on Medicus ICU as part of the Critical Care Minimum Dataset (CCMDS) is shared internally with finance departments for gathering Payments by Results (PbR) data used for commissioning purposes.
- Key analysis of unit data is made more readily available to managers and clinicians alike using various customisable dashboards. The dashboards provide extensive key indicators for a range of items such as general data, booked patients, SMR, adverse events, sepsis, infections, complications and more.
- Reporting is made easily available through the use of summary dashboard reports, a library of template reports and a custom report editor for the creation of bespoke ad hoc reports.

Additionally, the proposal is to develop a HL7 ADT Integration between Medicus ICU and the existing hospital PAS/EPR system provided by System C. This link will automate patient demographic, hospital and unit admission and discharge information for each patient into the entered into the Medicus ICU system. Automation of this

		<p>basic level of data proposes to save approximately 50 minutes of data entry time per day based on ICU activity data. Additionally, there is assumed to be a monthly time saving of approximately four hours for the generating of service audit and reporting data which will be made more readily available via template reports built into the Medicus ICU system alongside the ability to generate custom reports which currently are calculated alongside paper-based record keeping.</p> <p>Alignment with Trust Digital Strategy:</p> <p>The implementation of an integrated system links with the trust strategy and objectives to be an IT enabled organisation, supporting the effective use of digital technology to improve patient and staff experience. The use of “Digital by Default” should help the team to move away from paper-based handovers. The project is also in line with NHS Digital Strategy in utilising information to drive improvements in quality, efficiency and outcomes.</p> <p>Evidence for change:</p> <p>Following new requirements from ICNARC for the collection of mandatory data as part of their new national dataset the Trust has decided to assess the market and, following extensive meetings with providers and reference sites, have brought to consideration Mela Solutions who are an existing supplier of over 200 adult intensive care units nationally.</p>
--	--	--

<p>Q3</p>	<p>What is the nature of your relationship with the data subject (patient, staff) whose data will be used?</p> <p>For example, do you provide direct care to the data subjects, are they your patients?</p>	<p>Data collected within the software will be for all patient admissions to Intensive Care for the purposes of mandatory national data collection and reporting as well as local analysis of service information. The data subjects are cared for by the Adult Critical Care Unit.</p>
------------------	--	--

--	--

Q4	Individuals need to be told how their information is processed.	
	Have you consulted the data subject or their representative about using this data? If not, please explain why you haven't consulted them?	Intensive Care data collection for ICNARC purposes is done under a section 541. However, trust policy should remain in regard to normal data protection standards and will be addressed in the Trust privacy policy.
	Please provide details and an example of how this consent (if appropriate to rely on consent as a legal basis) to processing of their data was given? (Preferably embed document)	N/A because consent is not the legal basis.
	What information will you give individuals informing them of what you are doing with their data? ie this is consent to the processing of their personal data, not consent to treatment.	<p>N/A there is an existing section within the Trust Privacy policy that covers Section 251.</p> <ul style="list-style-type: none"> • To comply with Confidentiality Advisory Group approvals under Section 251 of the NHS Act 2006, this permits the collection of health information for patients with specific conditions without consent for the benefit of research and other important activities. Examples include the National Cancer Registry, the Trauma Audit and Research Network, the National Congenital Anomaly, Rare Disease Registration Service, and the NHS Patient Survey Programme. If you wish to opt out of your information being used for these purposes, please contact the Trust's Data Protection Officer. • When your information is used for your care and administrative purposes related to your care it is processed for the purposes of Article 6.1(e) of the GDPR – processing is necessary for the performance of a task carried out in the public interest and Article 9.2(h) of the GDPR – processing of special categories of data is necessary for the purposes of preventative or occupational medicine... [and] the provision of

		health or social care treatment or the management of health or social care systems and services.
	Is this information covered by our existing fair processing information or leaflet? If Yes, provide details. If No, please provide text to be added to our fair processing information. <u>Patient</u> ¹ <u>Staff</u> ²	N/A please see above.
	Explain why you believe they would consider the proposed new use of their data as being reasonable or expected?	Patients would expect that Data collection and analysis would be used to evaluate and improve services. This data use supports this process.


Q5	Has an assessment been made that the information collected is the minimum required to meet the aim of the project?	
	Use of data should not be the first resort if the objective can be achieved without its use. You must justify why the use of all the data is necessary and proportionate. For example, do you need to use all the fields, can you not achieve the same objective with fewer data fields and/or a smaller data set?	Data will be collected to cater for the mandatory Intensive Care National Audit & Research Centre (ICNARC) version 4 dataset and Critical Care Minimum Data Set (CCMDS). Data outside of these two minimum data collection standards are not required. All patient admissions to Intensive Care must be captured Local dashboards are generated using existing mandatory data fields. For further local quality improvement purposes additional data fields would only be added if unable to be collected in other/existing processes e.g. paper, and the minimum dataset collected.
	Has consideration been given to how the same objective or outcome may be achieved without using this data or using less data or employing a different method - explain in full?	Yes. Using less data would not be an option as there is a fixed mandatory requirement. Different methods, such as a manual process or in-house solution, would not offer the save efficiencies in terms of time savings or ready to use “out the box” solution. Local dashboards are generated using existing mandatory data fields; there is no alternative to collecting this data. Additional data fields would take the place

¹ <https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/>

² <https://www.sfh-tr.nhs.uk/work-for-us/your-staff-information/>

		of paper/ad hoc data collection processes that would otherwise take place.
--	--	--

Step 2: What type of data is being processed?

Q6 Fully describe ALL the data that will be used and justify why they are needed.	
Data item ie MRI images, patient, name, address, IP address, NHS/D number	Why is it necessary?
 Medicus Manual - ICNARC Data Collect	
All ICNARC version 4 data set fields (pdf file attached). 100+ fields including hospital number, patient demographic details, admission, diagnosis, discharge information and more.	National mandatory data collection requirement for benchmarking against other intensive care units in the UK for all patient admissions.
Local data – delirium incidence (national quality indicator), tracheostomy procedures	To comply with auditing of policy and guidelines this enables the identification of relevant patient cohorts

Q7 Will you use special categories of personal data?	
political opinions	<input type="checkbox"/>
racial or ethnic origin	<input checked="" type="checkbox"/>
religious or philosophical beliefs	<input type="checkbox"/>
trade-union membership	<input type="checkbox"/>
genetic data	<input type="checkbox"/>
biometric data for the purpose of uniquely identifying a natural person	<input type="checkbox"/>
data concerning health	<input checked="" type="checkbox"/>
data concerning a natural person's sex life or sexual orientation	<input type="checkbox"/>

Q8 Approximately how many individuals will be in the dataset?	
<11 individuals	<input type="checkbox"/>
11 – 50 individuals	<input type="checkbox"/>
51 – 100 individuals	<input type="checkbox"/>
101 – 300 individuals	<input type="checkbox"/>
301 – 500 individuals	<input type="checkbox"/>
501 - 1,000 individuals	<input type="checkbox"/>
1,001 - 5,000 individuals	<input checked="" type="checkbox"/>
5,001 - 10,000 individuals	<input type="checkbox"/>
10,001 - 100,000 individuals	<input type="checkbox"/>
100,001 or more individuals	<input type="checkbox"/>



Q9	How large and expansive are the records sets being used, what will it consist of?
	See attached ICNARC version 4 dataset. 100+ fields including hospital number, patient demographic details, admission, diagnosis, discharge information and more.

Q10	What geographical area will the data be drawn from or cover? For example, Mansfield, Ashfield, Newark and Sherwood patients. Derbyshire patients?
	All Intensive Care Unit admissions. Generally, the local area however in certain circumstances patients may attend from elsewhere including transfers from other hospitals or patients temporarily present in the region.

Q11	What is the source of this data?				
	<table border="1" style="width: 100%;"> <tr> <td style="width: 50%; vertical-align: top;"> <p>If the data is being taken from an existing system, identify what system that is and what was the originally purpose that data was collected for?</p> <p>How will this data be accessed?</p> </td> <td style="width: 50%; vertical-align: top;"> <p>System C – CareFlow PAS/EPR. Patient demographic, admission and discharge information collected as standard for all hospital admissions.</p> <p>Data will be transferred to the Medicus ICU system via standard HL7 ADT messaging.</p> <p>Remainder of data will be taken from patient notes/records (which are currently in paper format)</p> </td> </tr> <tr> <td style="vertical-align: top;"> <p>If it is new data/system that is being collected, describe how this data collection will be done i.e. digital, paper, removeable media?</p> </td> <td style="vertical-align: top;"> <p>Existing patient demographic, admission and discharge information will be automated into Medicus ICU from the System C – CareFlow PAS/EPR when creating a patient record and entering the patient’s hospital number. Data will be transferred to the Medicus ICU system via standard HL7 ADT messaging.</p> <p>Intensive Care specific treatment information will then be collected electronically via internet accessible devices, generally PC or laptop, by the ICU data collection audit team.</p> </td> </tr> </table>	<p>If the data is being taken from an existing system, identify what system that is and what was the originally purpose that data was collected for?</p> <p>How will this data be accessed?</p>	<p>System C – CareFlow PAS/EPR. Patient demographic, admission and discharge information collected as standard for all hospital admissions.</p> <p>Data will be transferred to the Medicus ICU system via standard HL7 ADT messaging.</p> <p>Remainder of data will be taken from patient notes/records (which are currently in paper format)</p>	<p>If it is new data/system that is being collected, describe how this data collection will be done i.e. digital, paper, removeable media?</p>	<p>Existing patient demographic, admission and discharge information will be automated into Medicus ICU from the System C – CareFlow PAS/EPR when creating a patient record and entering the patient’s hospital number. Data will be transferred to the Medicus ICU system via standard HL7 ADT messaging.</p> <p>Intensive Care specific treatment information will then be collected electronically via internet accessible devices, generally PC or laptop, by the ICU data collection audit team.</p>
<p>If the data is being taken from an existing system, identify what system that is and what was the originally purpose that data was collected for?</p> <p>How will this data be accessed?</p>	<p>System C – CareFlow PAS/EPR. Patient demographic, admission and discharge information collected as standard for all hospital admissions.</p> <p>Data will be transferred to the Medicus ICU system via standard HL7 ADT messaging.</p> <p>Remainder of data will be taken from patient notes/records (which are currently in paper format)</p>				
<p>If it is new data/system that is being collected, describe how this data collection will be done i.e. digital, paper, removeable media?</p>	<p>Existing patient demographic, admission and discharge information will be automated into Medicus ICU from the System C – CareFlow PAS/EPR when creating a patient record and entering the patient’s hospital number. Data will be transferred to the Medicus ICU system via standard HL7 ADT messaging.</p> <p>Intensive Care specific treatment information will then be collected electronically via internet accessible devices, generally PC or laptop, by the ICU data collection audit team.</p>				

Q12	How will this data be used?
------------	------------------------------------

	<p>Will this data be used or combined with other data sets, if so, what are these other data sets?</p>	<p>The Data set is not being combined with any other. All of the mandatory reporting takes a selection of the Data set.</p> <p>Both the ICNARC version 4 and CCMDS data sets have overlap for intensive care treatment information. Data collection is predominantly focused on the mandatory ICNARC data collection requirements however the CCMDS information is also contained within the software.</p> <p>The Critical Care Minimum Data Set was developed by the Critical Care Information Advisory Group (CCIAG) and endorsed by the Intensive Care Society.</p> <p>The Critical Care Minimum Data Set contains a subset of mandatory items for the generation of Critical Care Healthcare Resource Groups (HRGs).</p>
	<p>What will this data show you that is relevant to the project aim and purpose?</p>	<p>The purpose of the Critical Care Minimum Data Set is to provide a standardised set of data to support National Tariff Payment System, Healthcare Resource Groups, Resource Management, Commissioning and national policy analysis. The full Critical Care Minimum Data Set has been incorporated into and is consistent with the ICNARC (Intensive Care National Audit and Research Centre) data collection. It allows benchmarking of unit performance with other similar units nationally.</p> <p>The Critical Care Minimum Data Set has been developed to be used in all units where Critical Care is provided.</p>
	<p>Describe the access controls in place. Will the supplier also have access to the data?</p>	<p>Access to the software and data is username and password protected. Data is also locally hosted by the trust and the supplier (Mela Solutions Ltd.) will act solely as the support provider for the software itself.</p> <p>No access by Mela Solutions Ltd unless requested by trust IT or designated users for support purposes.</p>

<p>Complete the Account Management and Access Standard Operating Procedure³</p> <div style="text-align: center;">  Account Management & Acces </div>	<p>Embed the completed procedure</p> <div style="text-align: center;">  Medicus%20-%20A dult%20Critical%20C </div>
---	---

Q13	Describe proportionality measures.	
	<p>Explain how the processing achieves your purpose?</p>	<p>The purpose is to support National Tariff Payment System, Healthcare Resource Groups, Resource Management, Commissioning and national policy analysis. The data that is collected will inform all of these areas.</p>
	<p>Is there another way to achieve the same outcome, give details of alternatives you have rejected and provide the reasons why?</p>	<p>The same could be achieved by manually collecting the data via pen and paper or Microsoft Office tools. However, this would require excessive manual data entry, lead to natural human error, security risks, information governance risks, lack of credible audit or export (to ICNARC and finance) functionality among other reasons.</p> <p>Alternative software providers have been researched and it has been assessed are either unable to provide the same level of functionality or meet the required standards necessary.</p>
	<p>Please explain why a smaller amount of data cannot be used.</p>	<p>There is a minimum national mandatory data collection requirement for both ICNARC and CCMDS that must be catered for.</p>
	<p>Does the National Data Opt-Out apply (allows patients to opt out of their confidential patient information being used for research and planning)?</p>	<p>Yes</p>
		<p>No</p>
		<p><input checked="" type="checkbox"/></p>
		<p><input type="checkbox"/></p>

Q14	What is the duration of this processing? Is this one-off processing or will it continue for a specified period?
------------	--

³ <https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=13618>

	<p>Data may be analysed short term or long term for the purposes of service improvements, benchmarking against other hospitals or trusts, or individual research or analysis. Data will be collected for each patient during their intensive care unit stay only, however, data may very well be analysed post unit stay for audit purposes.</p> <p>There is reporting is currently ongoing and does not have an end point.</p>
--	---

Q15 How long will the data be kept and how will it be deleted?	
<p>NHS data needs to be retained in accordance with the Records Management Code of Practice⁴. You can check the schedule here⁵.</p> <p>Has provision been made to ensure you are able to accommodate this?</p> <p>If No, describe how the data will be managed.</p>	<p>Data will be collected and exported for mandatory reporting purposes. Following this point, data is retained locally by the trust within the software as per standard codes of practice (Records Management Code of Practice).</p> <p>ICNARC have their own retention policy which can be located here: https://www.icnarc.org/About/Information-Standards/Information-Security/Retention-Of-Records-Procedure</p>
<p>If data is being processed by a third party, how will we ensure data is deleted when required? Appropriate evidence would be an embedded copy of the contract or agreement containing this detail.</p>	<p>Yes, as shared within their privacy policy.</p> <p>https://www.icnarc.org/About/Information-Standards/Information-Security/Privacy-Policy</p>
<p>What will happen to the data at the end of the project/activity or end of contract with a third party? Will it be returned or deleted and how will this be done? Most contracts specify what happens to data at the end of contract. If this is not subject to contract, how will you ensure the data held by any third party is deleted? Embed extract of contract as necessary with highlighted sections.</p>	<p>Data will be extracted from the software as part of the removal of the system at the end of the contract. The supplier shall liaise with the trust around this process and ensure that all data is available.</p> <p>As per the contract:</p> <p><i>20.5 Within 10 Business Days following the termination of this Agreement, the Licensee shall:</i></p> <p><i>(a) return to the Licensor or dispose of as the Licensor may instruct all media in its possession or control containing the Software; and</i></p>

⁴ <https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8647>



⁵ <https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/#appendix-ii-retention-schedule>

		<p><i>(b) irrevocably delete from all computer systems in its possession or control all copies of the Software, 20.6 For the avoidance of doubt the Licensor shall extract all Licensee data held on the Software at termination or at the date stated in Part 3 of the Schedule, whichever is the earliest. The Licensee shall have access to remove such extracted data for 30 days from extraction. The Licensor will delete from the Software and all systems the Licensee's data once the 30 days have expired.</i></p>
--	--	--

Q16	Has the personal/special categories of data been minimised?	
	<p>Please explain why a smaller amount of data cannot be used and explain why all the data fields are necessary to achieve the objective. You are required to minimise the amount and level detail of any data set. For example, dates of birth should not be used where age would provide sufficient information to achieve the project aim.</p>	<p>Software is tailored to cater for the minimum requirements of data collection for the ICNARC version 4 dataset. Any reduction of data collected would result in failures to provide mandated standard requirements for valuable audit and research purposes.</p>
	<p>How will you prevent function creep?</p>	<p>Processes and functionality are regularly reviewed to cater for any changes in data collection requirements. ICNARC, as a governing body for Intensive Care data collection, inform software suppliers immediately of any changes in requirements which are then passed on to users via updates and upgrades within the software.</p>
	<p>How will you ensure high standards of data quality?</p>	<p>Firstly, the software is tailored to follow the data collection standards from start to finish via intuitive flow processes. Data collectors are trained both by the software supplier and the ICNARC research body in order to provide clarity on requirements. Before submission of completed data there are also auto prompts and data validation reports that highlight missed fields or inaccurate information.</p>

Q17	Is the data anonymised or pseudonymised in any way?	Anonymised	Pseudonymised
		<input checked="" type="checkbox"/>	<input type="checkbox"/>
	If the data is pseudonymised please describe how this has been done and 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.	Data will be exported and shared with ICNARC for mandatory national reporting, however, at this point data will be anonymised and coded.	
	If the data is pseudonymised describe how the data will be transferred ie using HL7. ie 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.	N/A.	
	Have you considered whether using anonymised/pseudonymised data is a suitable alternative, please explain how this has been considered and why it is not suitable?	<p>All data collected is either mandatory or of value. For national collection the Data will be exported and shared with ICNARC for mandatory national reporting, however, at this point data will be anonymised and coded.</p> <p>For local audit purposes data will be pseudonymised on the system, and export of data/analysis in anonymised.</p>	
	What steps have been taken to minimise the risk of re-identification of anonymised or pseudonymised data?	IG mandatory training for users. Restricted (role based) access to system. Anonymised exports	

Step 3 – Data security

Q18 Where will the data be stored?			
Will the data be stored on our servers or servers/cloud external to the Trust?			
Internal	External	Server	Cloud*
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
If external, where will it be stored, will this be the UK, EU/EEA or elsewhere? Provide the location/country ie London, England		N/A.	
If the data is processed outside of the EU/EEA, what safeguards will be in place?		N/A.	
If a supplier is used, they must complete the supplier assurance framework below. <div style="text-align: center;">  Supplier Assurance Framework TEMPLATE </div>		N/A	
Will the storage be controlled by another party (not the supplier) such as a product/ platform supplier ie AWS, Google, Microsoft? Provide details.		Data stored on dedicated local trust server. The software uses https, so no client needed. 19/01/24 Software cyber tested - no vulnerabilities detected above a 7.5 so passes.	
If the data is stored on the cloud the following assessment must be completed by the supplier <div style="text-align: center;">  Cloud Assessment.xlsx </div>		N/A.	
If the data storage or processing is being done by a supplier, what certifications do they hold?			

When were they, and the proposed storage mechanism, subjected to an external penetration test and is a report available? (Please embed any documentary evidence)			
	Certificate	External Penetration Test undertaken (date)	External Penetration Test Report
Cyber Essentials +/- Cyber Assessment Framework (CAF)	Yes - Certificate number; b5c7f838-bbc8-4c51-846a-bc36a2cfb72b		
ISO 15489 Records Management	No		
ISO 27001 Information Security Standards	No		
ISO/IEC 27701:2019 Ext to 27001/27002	No		
ISO 27017 Cloud Services	N/A		
ISO 27018 PII in public clouds	N/A		
Digital Technology Assessment Criteria for Health and Social Care (DTAC)	No		
ISO 9001 Quality Management Systems	No		
Other, please specify.			
If a supplier is used, are they registered with the ICO. Check the register ⁶ and provide the certificate number.	Yes	No	
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Registration reference: Z8172745		
If a supplier is used, have they completed the Data Security and Protection Toolkit, search the register here ⁷	Yes	No	N/A
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

⁶ <https://ico.org.uk/ESDWebPages/Search>

⁷ <https://www.dsptoolkit.nhs.uk/OrganisationSearch>

	If yes, complete the following	Organisation code	Status	Date Published	
		8JK86	Standards Exceeded	03/07/2023	
	Security of ICT been evaluated	Yes - Carried out by external organisation through penetration testing			
	Processes in place to ensure business continuity management arrangements are tested and reviewed?	Yes - Tested and reviewed in last 12 months			

Q19 How will this data be secured during storage and when being moved?	
Will it be encrypted when stored and/or moved, if so what type of encryption will be employed?	<p>Data at REST is defined as data in archived form and is encrypted on a dedicated Mela Solutions server using Bitlocker.</p> <p>Mela Solutions Ltd ensures that authentication credentials transmitted to network devices are encrypted in transit.</p> <p>All source code and build instructions are backed up daily and the backups are held encrypted in a physically separate data centre.</p>
Will it be on a server protected by firewall and network intrusion detection?	Yes.
What technical controls are in place to prevent hacking of the data by unauthorised persons?	Technical controls and secure communication protocols are implemented to prohibit unrestricted connections to untrusted networks or publicly accessible servers.
When being moved will it be secured through encrypted file transfer, secure transmission through SLL/TLS/SHS, please explain the specific technical standards that will apply?	SSL used to encrypt end to end communication of data.
Do you have a business continuity plan for the information?	Yes. See attached. Essentially the system failure is reported to NHIS, and data is collected on paper/manually until system restoration at which point it is entered retrospectively.

		<u>Action Card for Nurse In Charge Loss of network information systems - MedicUS</u>		
	What types of backups are undertaken i.e. full, differential or incremental?	Full	Differential	Incremental
		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Q20	Who will have access to this data and how will this access be controlled?		
	Will the data be kept on a system that is password controlled, what is the password length and how often does it have to be changed? Who will administer these access controls?	Locally hosted system with dedicated user defined administrators. Password strength, length, frequency of change and number of unique sequential passwords can all be configured by the administrators. <u>This will be in line with SFH policy.</u>	
	Is there an ability to audit access to the information? Can the supplier audit our data?	Supplier can audit activity logs upon authorised user request.	
	What other security measures are in place, such as physical security, smartcard, Active Directory, multiple factor authentication?	Two factor authentication soon to be implemented.	
	Is training available to staff for the new system?	Yes	No
		<input checked="" type="checkbox"/>	<input type="checkbox"/>

Q21	If you are using devices such as laptops to access data, how are these secured and managed?		
	Browser based software only accessible within the trust network. Access to the system is username and password restricted. All laptops are also username and password restricted.		

Q22	Is this data an attractive target for criminals and hackers; does it contain information that may be used for identity/financial fraud or reveal a person possibly being vulnerable to exploitation?	
	Yes <input type="checkbox"/>	No <input checked="" type="checkbox"/>




	<p>Rate its attractiveness from 0 to 10 below. https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime</p> <p>Choose an item.</p> <p>If this is a risk describe how you will manage it in stage 8.</p>	
--	--	--

Step 4 – Data use and sharing

Q23	Will this data be shared with anyone else?	
	If yes, explain who these other parties are and why the data is being shared?	Yes. Data will be exported and shared with ICNARC for mandatory national reporting, however, at this point data will be anonymised and coded.


Q24	Are other people processing this data?	
	If a third party such as a company is storing or otherwise managing or using our data, please explain what they doing and why they are doing it?	<p>ICNARC manage the Case Mix Programme (CMP) which is an audit of patient outcomes from adult, general critical care units (intensive care and combined intensive care/high dependency units) covering England, Wales and Northern Ireland. The CMP is included in the NHS England Quality Accounts List, which is overseen by the Health Quality Improvement Partnership (HQIP), meaning that it is a national clinical audit that Trusts are recommended to take part in.</p> <p>Currently 100% of adult, general critical care units participate in the CMP. Other specialist units, including neurosciences, cardiac and standalone high dependency units, also participate.</p> <p>The CMP is open to both NHS (publicly funded) and independent sector critical care units.</p> <p>Critical care units collect data on all the patients they admit to their unit. They securely submit these data and the CMP team run over 600 validation checks, identifying errors and missing information. Units then have a chance to correct and complete the data before analyses.</p> <p>The unit then receives cumulative Quarterly Quality Reports (QQRs) which show how the unit compares to other units identified as receiving similar types of admissions and all units in the CMP. The reports focus on a set of key potential quality indicators, and</p>

		<p>identify trends over time, helping the unit to understand more about the care they deliver. The aim is to assist the unit in decision-making, resource allocation and local quality improvement.</p> <p>With over 3 million patients in the database, the CMP provides the backbone for several important research studies and is a useful resource for many types of data analysis. ICNARC also publish the CMP Annual Quality Report. This publicly available report compares the risk-adjusted mortality and key quality indicators at various levels (for critical care units, hospitals and trusts), for the period 1 April to 31 March annually.</p>
	<p>If we are using a third-party product that requires maintenance where they access our networks, explain how this will be managed (will they remotely connect, how will this access be managed).</p>	<p>N/A</p>
	<p>Is there a process in place to remove personal data if data subject refuses/removes consent? ie The right to restrict processing/the right to object - People can request the use of their data to be restricted in certain circumstances. These will be considered on a case-by-case basis.</p>	<p>Software can cater for and follow the trust policy.</p>
	<p>Are arrangements in place for recognising and responding to requests for access to personal data?</p>	<p>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)</p>

<p>Q25</p>	<p>Describe the data flows</p>	
	<p>Please complete the data flow template below to detail how the data is collected, moved and used?</p> <div style="text-align: center;">  New Flow Map UPDATED.xlsm </div>	<div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  Medicus Manual - </div> <div style="text-align: center;">  Medicus - HL7 PAS </div> </div> <p>ICNARC Data Collect Link Spec - ICNARC \</p> <p>Data is collected in Medicus ICU via the patient data flow informed by ICNARC version 4 (attached). HL7 messaging from the System C (CareFlow) PAS/EPR</p>

		<p>automates data for any patients created on the Medicus ICU system.</p> <p>All data is then held on the Medicus ICU system which is stored locally on a trust hosted server.</p>
	<p>Are there security or data protection concerns in any of the data flow stages you identify? If so, please indicate where and what steps you taking to reduce this risk?</p>	N/A.

Step 5 – Processing by or with a supplier/third party

Q26	If you are using a supplier or organisation to process, store or otherwise interact with this data, if not answer N/A	
	<p>What is the arrangement between the Trust and the supplier/third party concerned?</p>	<p>Mela Solutions Ltd. provides and supports the Medicus ICU software through the provision of an App. All data stored on the app is held on the Trust Server behind firewalls. Mela Solutions Ltd will only have access data when approved by the Trust.</p>
	<p>What activities will the supplier/third party carry out i.e. storage, transport, processing of data on their platform</p>	<p>Mela Solutions Ltd will only access the server to carry out updates and will not store transport or process data without Trust permission.</p>
Q27	<p>What steps or measures will you put in place to manage these risks? What measures will you take to ensure processors comply? PLEASE ATTACH COPIES/ RELEVANT SECTIONS OF ANY CONTRACT/ AGREEMENT.</p>	<div style="text-align: center;">  Mela Solutions - Software Licence Ag </div>

Step 6 – Consultation

Q28	Consider how to consult with those who have an interest in this project	
	Describe when and how you will seek individuals' views or justify why it's not appropriate to do so. ie do we need wider public engagement.	The DPIA will be forwarded to the Information Governance Working Group for wider stakeholder engagement.
	Who else do you need to involve within the Trust? ie Digital Innovations Approval Group (DIAG).	DIAG. IT/Integrations.
	Do you need to ask the data processors (supplier) to assist?	Yes. For installation, integration development, training and support.
	Do you plan to consult information security experts, or any other experts?	N/A.

Step 7 – Lawful basis

Q29	What is your lawful basis for processing personal data? Select all that apply	
	a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes. Please note, do not use this if it is for direct care, (e) maybe more appropriate	<input type="checkbox"/>
	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	<input checked="" type="checkbox"/>
	c) processing is necessary for compliance with a legal obligation to which the controller is subject	<input checked="" type="checkbox"/>
	d) processing is necessary in order to protect the vital interests of the data subject or of another natural person	<input checked="" type="checkbox"/>
	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	<input checked="" type="checkbox"/>

Q30	What is your lawful basis for processing special categories of personal data? Select all that apply	
	a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes. Please note, do not use this if it is for direct care, (h) and/or (i) maybe more appropriate	<input type="checkbox"/>
	b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment	<input type="checkbox"/>
	c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent	<input type="checkbox"/>
	e) processing relates to personal data which are manifestly made public by the data subject	<input type="checkbox"/>
	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	<input checked="" type="checkbox"/>

	i) processing is necessary for reasons of substantial public interest, ie public health, such as protecting against serious cross-border threats to health	<input type="checkbox"/>
	j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purpose	<input checked="" type="checkbox"/>

Stage 8 – Risk Template

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

Completed by: Vishal Dhokia

Role: Speciality Head of Service

Date completed: 07/03/2024

Guidance notes:

Confidentiality - Are there any risks to the confidentiality of personal data? Do staff have a legitimate relationship in order to process personal data? Is personal data disclosed to people who do not require it?

Integrity - Systems must be designed so that the input and management of information is not prone to human error and that the flow of information does not result in loss or alteration. Data should be complete and accurate and not tampered with during or after submission. Ensuring that during the process of transmission data integrity is maintained.

Availability - System design must include appropriate access controls and checks, so that the information in the system has consistency, accuracy, can be trusted as correct and can be relied on when providing healthcare. Data is available and delivered to the right person, at the time when it is needed and that there is accessibility to systems at all times. Having safeguards in place for power outages, natural disasters, hardware failures and systems upgrades.

Examples of risks that are common in projects is included below. Please amend/delete as necessary.

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)	
<p>Clinical critical data is absent because it is not recorded.</p> <p>Critical data not entered in the system, e.g. because admin/clinician is not prompted or forgets to record it.</p> <p>Incorrect or missing values will lead to wrong conclusion from the clinical audit.</p> <p>Time lost from inputting and correcting inaccurate information in the first instance.</p> <p>This may lead to delayed or inaccurate submissions to ICNARC resulting in minor reputational</p>	<p>Intuitive headings and fields to prompt users to capture critical data and key clinical information.</p> <p>Integrations with third party systems to reduce manual data entry.</p> <p>Data validation reports in order to verify missing or incorrect information.</p> <p>Training users via meetings and support documents on data entry best practice.</p> <p>Regular updates from supplier to advise users of any planned upgrades and a process is in place to contact all main users for support during any unplanned downtime.</p> <p>User training from Mela Solutions for clarity and</p>	2	2	4		2	2	4	

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)	
damage / regulatory action	<p>understanding of software functionality.</p> <p>Training with ICNARC for awareness and knowledge of data entry requirements.</p> <p>Customer support and helpline.</p>								
<p>Clinical professionals may want to record information in a different format i.e. use free text to record additional detail rather than follow the structured options.</p> <p>Causes may be lack of familiarity with the data collection format or assumptions based on past experience rather than current processes.</p>	<p>Free text, although acceptable and needed, should be limited to the additional description of fixed items already selected.</p> <p>Guidance provided on what should be recorded under each heading and extensive provision of text boxes attached to most key fields.</p> <p>Induction training from both the software supplier (Mela Solutions) and ICNARC for the national data collection.</p>	2	2	4	User familiarity with the correct structure and processes toward recording accurate and validated data.	2	1	2	Training to ensure all users are familiar with the correct structure and processes toward recording accurate and validated data

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)	
<p>Important information may therefore be omitted.</p> <p>This may lead to inaccurate submissions to ICNARC resulting in minor reputational damage / regulatory action.</p>	<p>Supporting material in the form of written documentation.</p> <p>Delivery of induction training from both the software supplier (Mela Solutions) and ICNARC for the national data collection.</p> <p>Providing supporting material in the form of written documentation.</p> <p>Awareness provided to all users of availability of on-going support and training.</p>								
<p>Data is accessed inappropriately due to improper access controls and permission. Movers and leavers access not removed. Data is inappropriately viewed, edited and/or disclosed.</p>	<p>Username, password and permission controls in place. Access is managed within the ICU Audit team. Account Management and access procedure to be audited on a regular basis. Appropriate access according to role. IG Training in place.</p>	2	2	4		2	2	4	

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)	
This may lead to minor reputational damage / regulatory action	Audit activity is available for user access upon request from the supplier (Mela Solutions).								
Potential issue with interface between Medicus ICU and System C – CareFlow PAS/EPR causing delays in data being updated on the software. This may lead to delayed or inaccurate submissions to ICNARC resulting in minor reputational damage / regulatory action	Regular updates from IT/Integrations team to advise Medicus ICU users of any planned updates and process to contact all main users for support during any unplanned downtime. Back-up (manual) process in place if the integration stalls or fails	2	2	4		2	2	4	IT/Integrations team and supplier.
System down time due to server failure. This may lead to delayed submissions to	Reporting structure between trust IT/Integrations team and Medicus ICU users for any in-house server hosted issues.	2	2	4		2	2	4	

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)	
ICNARC resulting in minor reputational damage / regulatory action	Supplier (Mela Solutions) support available during Monday – Friday 9:00am – 17:30pm. Business continuity plan in place.								
Personal data not being encrypted both/either in transit or at rest. This may lead to minor reputational damage / regulatory action	HTTPS/SSL encrypted connection.	1	1	1	N/A	1	1	1	Mitigated upon installation and configuration pre go-live.



Risk Scoring
Matrix.pdf

Step 8 – Legal compliance

To be amended by Information Governance from the responses provided in the previous stages.

UK General Data Protection Regulation 2018	Compliance
<p>Principle 1 – Personal data shall be processed fairly and lawfully and, in a transparent manner.</p>	<p>Lawfulness</p> <ul style="list-style-type: none"> • 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. <p>Fairness</p> <ul style="list-style-type: none"> • 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. <p>Transparency</p> <ul style="list-style-type: none"> • We are open and honest and comply with the transparency obligations of the right to be informed.
<p>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.</p>	<ul style="list-style-type: none"> • 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.

	<ul style="list-style-type: none"> • 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.
<p>Principle 3 – Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.</p>	<ul style="list-style-type: none"> • We only collect personal data we actually need for our specified purposes. • We have sufficient personal data to properly fulfil those purposes. • We periodically review the data we hold and delete anything we don't need.
<p>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.</p>	<ul style="list-style-type: none"> • 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
<p>Principle 5 – Kept no longer than is necessary.</p>	<ul style="list-style-type: none"> • 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 three Inquiries including the Goddard Inquiry, no destruction or deletion of patient records is to take place until further notice. • We clearly identify any personal data that we need to keep for public interest archiving, scientific or historical research, or statistical purposes.

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.
- When deciding what measures to implement, we take account of the state of the art and costs of implementation.
- We have an information security policy and take steps to make sure the policy is implemented.
- When deciding what measures to implement, we take account of the state of the art and costs of implementation.
- We make sure that we regularly review our information security policies and measures and, where necessary, improve them.
- We have assessed what we need to do by considering the [security outcomes](#) we want to achieve.
- We have put in place technical controls such as those specified by established frameworks like Cyber Essentials.
- We understand that we may also need to put other technical measures in place depending on our circumstances and the type of personal data we process.
- We use encryption and/or pseudonymisation where it is appropriate to do so.
- 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.
- Where appropriate, 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.

Principle 7 – Accountability principle

- We take responsibility for complying with the UK GDPR, at the highest management level and throughout our organisation.
- We keep evidence of the steps we take to comply with the UK GDPR.
- We put in place appropriate technical and organisational measures, such as:
 - adopting and implementing data protection policies (where proportionate).
 - taking a ‘data protection by design and default’ approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations.
 - putting written contracts in place with organisations that process personal data on our behalf.
 - maintaining documentation of our processing activities.
 - implementing appropriate security measures.
 - recording and, where necessary, reporting personal data breaches.
 - carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals’ interests.
 - appointed a data protection officer; and
 - adhering to relevant codes of conduct and signing up to certification schemes (where possible).
- We review and update our accountability measures at appropriate intervals.

Step 9 - Assessment Summary

To be completed by Information Governance.

Outcome of Data Protection Impact Assessment	
Project is not recommended to proceed, as significant risks have been identified.	<input type="checkbox"/>
Project to proceed once identified risks have been mitigated as agreed.	<input type="checkbox"/>
Project has met required legislative compliance and poses no significant risks. No further action required.	<input checked="" type="checkbox"/>

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks.	
Legislative Compliance:	<p>Suggested text, remove, amend as necessary.</p> <p>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.</p> <p>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)</p> <p>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.</p>
Summary of Risks	<p>Suggested text, remove, amend as necessary.</p> <p>Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management.</p>
Identified risks.	
The risk	Mitigation
Loss of system access	Full system back-up process in place

Loss of system data	Full system back-up process in place
Data is accessed inappropriately	individual username and passwords are provided. There is a risk of unauthorised access due to the system being unable to report on users that have accessed individual patient records

Step 10 - Recommendations for Action

Summary of recommendations (amend/delete as necessary)		
Recommendations	Recommendations	Agreed deadline for action
Information Asset Administrators to ensure Medicus is added to the information asset register and data flows are mapped and recorded.	IAO/IAA	Complete for March 2024
Account management Standard Operating Procedure generated and implemented, routine audit to take place.	IAO/IAA	SOP complete Review date March 2025

Step 11 - Project signoff

	Name	Job Title	Date
Information Asset Owner*	Vishal Dhokia	Speciality Head of Service	08/03/2024
Data Protection Officer	Jacque Widdowson	Head of Data Security and Privacy	08/03/2024
Senior Information Risk Owner	Sally Brook Shanahan	Director of Corporate Affairs	08/03/2024
Caldicott Guardian	David Selwyn	Medical Director	08/03/2024
Chief Digital Information Officer	Paul Moore	Acting Chief Digital Information Officer	12/03/2024
Patient safety⁸			

The Data Protection Impact Assessment must be reviewed and approved by the Information Asset Owner, Data Protection Officer, Senior Information Risk Owner and Caldicott Guardian. Approval does not close the data protection risks related to this project.

*It is important that the risks and the original scope of the project are reviewed on a regular basis to ensure any new confidentiality, integrity or availability risks are identified, documented, and mitigated wherever possible. All amendments must be approved following the approvals process.

⁸ [DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital](#)