

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?.....	9
Step 3 – Data security.....	15
Step 4 – Data use and sharing	19
Step 5 – Processing by or with a supplier/third party	20
Step 6 – Consultation	21
Step 7 – Lawful basis.....	22
Stage 8 – Risk Template	24
Step 8 – Legal compliance	27
Step 9 - Assessment Summary.....	31
Step 10 - Recommendations for Action.....	32
Step 11 - Project signoff	33

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 \(notts.nhs.uk\)](https://www.notts.nhs.uk)

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

Project title:	Nottingham and Nottinghamshire LMNS CardMedic Pilot.
Reference number:	
Implementing organisation:	Sherwood Forest Hospitals NHS Foundation Trust
Key contacts involved in the DPIA (name and job title)	Siobhan Buxton – Maternity Commissioning Manager Nottingham and Nottinghamshire ICB. Gemma Boyd – Consultant Midwife (SFH). Debrah Neale – Matron for Community Engagement and Innovation (NUH) Claire Madon – Chief Nurse Information Officer (SFH)
Information Asset Owner (name and job title)	Siobhan Buxton ICS Gemma Boyd SFH Debrah Neale NUH
Information Asset Administrator (name and job title)	As above

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>To improve interpreting, translation and quality information given to women and birthing people whose first language is not English CardMedic is being piloted for a 12-month pilot phase for use in the Maternity and Neonatal settings across the LMNS in Nottinghamshire.</p> <p>The use of CardMedic aims to reduce health inequalities, offer patient centred care, enhance quality of care, and improve patient safety.</p> <p>CardMedic is an innovative digital communication tool designed to improve the transfer of vital information between healthcare staff and patients, across any barrier – including language barriers; visual, hearing, or cognitive impairment, or PPE. CardMedic has an A-Z digital platform of flashcards with pre-written scripts replicating clinical conversations around common</p>
-----------	--	--

		<p>healthcare topics and live chat function which can translate in verbal and written format.</p> <p>The A-Z collection of digital flashcards is available in over 1200 medical topics and translates into 40+ languages. It replicates conversations around common health care topics with simple questions and explanations to guide the clinical interaction.</p> <p>CardMedic work alongside trusts to co-create specific processes and procedures to ensure the content library meets the needs of their service. Content is tested on patients to ensure it is easily understood. Due to CardMedic working alongside healthcare organisations the library and languages are always expanding. As a subscriber to this service, we have direct input to any changes or new content creation. We will work closely with Maternity Voices and Neonatal Voices Leads locally when creating any new content.</p> <p>CardMedic is device agnostic and can be accessed using a mobile phone, tablet or desktop. The tool can also be used offline. The use of IPADS, computers on wheels and iPhone are commonly used by staff in maternity and neonatal services across the LMNS which will support the use of this tool.</p> <p>Maternity and Neonatal staff working at NUH and SFH will be forwarded a registration email to register to CardMedic by an internal member of staff. This is a one-off process to enable a login to the application.</p> <p>The member of staff can then choose if they wish to sign up and provide their personal data to have access to the CardMedic system.</p> <p>Newly registered user data described above (name, occupation, registration date and email address) are sent via password protected spreadsheet via email to an</p>
--	--	---

		agreed point of contact in SFH/NUH (and subject to Data Sharing Agreement).
--	--	---

Q2	<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>Communication barriers can lead to health inequalities and can occur from physical barriers (PPE), language barriers and those with communication difficulties (such as cognitive impairment, learning difficulties and autism).</p> <p>There is a wealth of evidence that associates language barriers with adverse events when accessing healthcare services and pregnant women who do not speak English are at greater risk of poor birth outcome compared to their English-speaking counterparts¹². Poor communication can also have a negative impact on a women's experience³.</p> <p>Expected Benefits.</p> <ul style="list-style-type: none"> • Improved communication between maternity and neonatal staff and families using the services. • Reduction in communication barriers and potential service gaps as a result at the point of care. • Enhanced experience for service users whose first language is not English. • Improve equity for all those using services. • Improve pregnancy outcomes and experiences for women whose 1st language is not English. • Will ensure that families are being catered for equally irrespective of the language they speak. • Improve confidence in the service provided to those who do not speak English. • CardMedic can be accessed easily in a variety of different settings including home, clinic, neonatal units, labour, and maternity wards. Is
-----------	--	---

¹ [s12939-021-01570-8.pdf](#)

² [Maternal Language and Adverse Birth Outcomes in a Statewide Analysis - PMC \(nih.gov\)](#)

³ [British Journal Of Midwifery - The importance of language in maternity services](#)

		<p>always available when a human interpreter isn't available.</p> <ul style="list-style-type: none"> • Improves access to care. • Provides consistent information. • Offer patients a personal experience by adding localised information such as discharge information, meals available and ward environment. • Improved relationship between healthcare professional and the service user.
--	--	--

Q3	<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>Commissioning manager completing DPIA on behalf of all partners. Staff members to support direct care to patients.</p>
-----------	--	---

Q4	Individuals need to be told how their information is processed.	
	<p>Have you consulted the data subject or their representative about using this data? If not, please explain why you haven't consulted them?</p>	<p>The data subject is staff working in maternity and neonatal services across the Nottingham and Nottinghamshire LMNS footprint.</p> <p>The initial data will be staff email address. All staff will then be forwarded a registration email by an administration member of staff within each Trust. It is staff choice to register to use the application.</p>
	<p>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)</p>	<p>Users are emailed details of how to register (by an administration member of staff when first using the CardMedic system if they wish to use this product. There is no requirement for staff to register, CardMedic is an additional resource to support current interpretation services.</p>
	<p>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>	<p>The registration email will provide staff with information on how their data will be stored and processed whilst using the CardMedic System.</p> <p>Please see privacy policy.</p>

		Privacy & Cookie Policy (cardmedic.com)
	<p>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.</p> <p>Patient⁴ Staff⁵</p>	<p>No</p> <p>Processing is consent SFH is not sharing any data as Data Controller.</p>
	<p>Explain why you believe they would consider the proposed new use of their data as being reasonable or expected?</p>	N/A

Q5	Has an assessment been made that the information collected is the minimum required to meet the aim of the project?	
	<p>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?</p>	<p>The system does NOT use or store any patient information. NO health information is stored. Staff/User data IS stored.</p> <p>The system holds the registration information for the user, this includes,</p> <ul style="list-style-type: none"> • Name – Account Management and identification of staff member. • Email address – Account Management and identification of staff member. • Place of work – Account Management and identification of staff member. • Occupation – For patients understanding of who they are communicating with. • Preferred language – Functionality. • Photo ID (optional) For patients understanding of who they are communicating with. <p>Staff will be forwarded details on how to register to CardMedic. It is staff choice to register if they wish to provide more personal data than the minimum requirement for this project.</p>

⁴ <https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/>

⁵ <https://www.sfh-tr.nhs.uk/work-for-us/your-staff-information/>

	<p>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?</p>	<p>The compulsory fields are the minimal data required to support the use of the CardMedic System with the optional photo field.</p>
--	--	--

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?
Staff Email Address	<p>Maternity and Neonatal staff working at NUH and SFH will be forwarded a registration email to register to CardMedic by an internal member of staff. This is a one-off process to enable a login to the application.</p> <p>SFH or NUH will not be sharing staff emails with CardMedic. CardMedic will only receive this information when a staff member chooses to register with them.</p>
Name	<p>Account Management and identification of staff member Data is processed to allow the registration of service users to ensure only authenticated and authorised access is provided to the CardMedic system.</p> <p>Lawful basis for processing is Consent. Staff members consent to data processing when registering with the CardMedic system.</p> <p>Users are subject to legally approved Terms and Conditions.</p> <p>The registration process uses AWS Cognito identity services and is based on the OAuth2 framework.</p> <p>Registered users can change their profile at any time. Users wishing to withdraw their account can do so by emailing the support desk, a link is provided on their profile settings.</p> <p>No other data subject is stored in the CardMedic system.</p>
Place of Work	Account Management and identification of staff member

	Occupation	For patients understanding of who they are communicating with.
	Preferred Language	Functionality.
	Users are also able to upload a picture of themselves	So that patients can confirm who they are talking to. This is optional and determined by the staff member.


Q7	Will you use special categories of personal data? no	
	political opinions	<input type="checkbox"/>
	racial or ethnic origin	<input 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 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	YES
	501 - 1,000 individuals	<input type="checkbox"/>
	1,001 - 5,000 individuals	<input 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?	
	The Record sets being used is what is outlined in Q6.	

Q10	What geographical area will the data be drawn from or cover? For example, Mansfield, Ashfield, Newark and Sherwood patients. Derbyshire patients?	
	Staff who work in maternity and neonatal services at Sherwood Forest Hospitals and Nottingham University Hospitals.	

Q11	What is the source of this data?	
	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?	Staff will be forward the registration email via administration staff in each department. These email addresses will be taken from internal circulation list.
	How will this data be accessed?	
	If it is new data/system that is being collected, describe how this data collection will be done i.e. digital, paper, removeable media?	N/A

Q12	How will this data be used?	
	Will this data be used or combined with other data sets, if so, what are these other data sets?	No
	What will this data show you that is relevant to the project aim and purpose?	The data used is to set up a staff account to use the app. The aim of the project is to improve the communication between staff member and patient.
	Describe the access controls in place. Will the supplier also have access to the data?	<p>This data is stored in a secure database within the Amazon Web Services infrastructure and not shared outside of the CardMedic system. No registration data is stored on any CardMedic device.</p> <p>The registration process uses AWS Cognito identity services and is based on the OAuth2 framework.</p> <p>Siobhan MacDonald (Head of Client Services at CardMedic) and Tim Grimaldi (as Siobhan's 'stand in' when she is unavailable) have access to registered user data. Data is limited to user's name, email address, occupation, organisation and date of registration. We have no access to their image files, nor to the card usage data per user. We store no patient data.</p>
	Complete the Account Management and Access Standard Operating Procedure ⁶	 ig-0121-account-management-and-acce

Commented [RG(FHNFT1)]: Need to upload the new version and convert to writeable PDF

⁶ <https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=13618>

Q13 Describe proportionality measures		
Explain how the processing achieves your purpose?	The Data which is provided to CardMedic allows staff to register and use the functionalities of the app, in order to improve communication with patients.	
Is there another way to achieve the same outcome, give details of alternatives you have rejected and provide the reasons why?	Google translate can be used to support translation, but it is recommended it should be avoided in healthcare settings as there is no assurance of the quality of translations.	
Please explain why a smaller amount of data cannot be used.	Minimal data is used to register the users to a CardMedic account.	
Does the National Data Opt-Out apply (allows patients to opt out of their confidential patient information being used for research and planning)?	Yes	No
	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Q14	What is the duration of this processing? Is this one-off processing or will it continue for a specified period?
	It will continue of the 1-year pilot period from 5 th February 2024 – 4 th February 2025. During the pilot evaluations will be done to determine whether it will be recommended for future use in maternity and neonatal services.

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 Practice⁷. You can check the schedule here⁸.</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 required is for the registration of staff to use the CardMedic System. This will allow them full access to CardMedic.</p> <p>Once the pilot is finished staff will no longer be able to access the full version of the Cardmedic system but will have access to the basic version.</p> <p>Users wishing to withdraw their account can do so by emailing the support desk. The Ts</p>

⁷ <https://www.sfh-tr.nhs.uk/about-us/policies-and-procedures/non-clinical-policies-procedures/information-governance/?id=8647>

⁸ <https://transform.england.nhs.uk/information-governance/guidance/records-management-code/records-management-code-of-practice-2021/#appendix-ii-retention-schedule>

		& Cs inform the user that they can delete their user registration. Please ask them to contact support@cardmedic.com for such requests.
	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	The Data is being sub processed by Amazon Web Services (AWS).
	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.	Name: CardMedic ID: 652876910361 CardMedic AWS compliance with NHS Data Security and Protection Toolkit: Amazon Web Services (AWS) - National Health Service (NHS) Data Security and Protection Toolkit (DSPT)

Commented [DJ(FHNFT2): Could a copy of the contract between AWS and CardMedic be provided for assurance. Which can then be embedded into this document.

Commented [BS(NANI53R2): CardMedic are in the process of accessing this contract

Commented [DJ(FHNFT4R2): Discussed with JW as the lawful processing of this data is consent and Staff are providing their own data to CardMedic and this is not being provided by SFH. Additionally staff do not need to sign up to this service. Although we are still awaiting for sight of the contract between Cardmedic and ASW we do not feel it needs to delay the progress of this DPIA.

Commented [DJ(FHNFT5): The contract between AWS and CardMedic needs to be viewed to answer this.

It also needs to be decided if SFH will continue to use the free version after the pilot.

Q16	Has the personal/special categories of data been minimised?	
	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.	Minimal data is used to register the users to a CardMedic account. Email Address – to send registration email. Name and Photo (if added by user) – to be used on the Hello Flashcard Place of work and Occupation – will support analytics and provide identification of the staff member to patients. Preferred language – can change CardMedic System to this language.
	How will you prevent function creep?	The only function creep possible would be to use CardMedic in other departments without IG/Strategic input. Sherwood Forest Hospitals (SFH) process for any new digital system would need to go through the DIAG, IGWG and IG Committee before being implemented.

	<p>How will you ensure high standards of data quality?</p>
	<p>Registration email to be sent internally (SFH).</p>

Q17	Is the data anonymised or pseudonymised in any way?	Anonymised	Pseudonymised
		<input 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.		
	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.	<p>Newly registered user data described above (name, occupation, registration date and email address) are sent via password protected spreadsheet via email to an agreed point of contact in SFH/NUH (and subject to Data Sharing Agreement). There is no patient data in these files and other than the user's email address, the remaining data is not personal and is public knowledge. If you require transfer of this data via another means and/or if you require a greater level of encryption for this data, please let us know as soon as possible.</p>	
	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>The Staff members name cannot be anonymized as this is used in a flash card for introductions with patients</p>	
	What steps have been taken to minimise the risk of re-identification of anonymised or pseudonymised data?		





Commented [CC(FHNFT6)]: Does this mean CardMedic sends the list of data they gather from the staff back to SFH or NUH? Why?

Commented [BS(NANIS7R6)]: This information is to
 - monitor uptake of the CardMedic app in their organisation,
 - to optionally request CardMedic end user feedback and/or
 - to optionally request specific engagement from CardMedic end users.

Will this cause a delays agreeing to the DPIA?
 The data sharing agreement will need signing and can be embedded within this document.


Commented [CC(FHNFT8R6)]: That's fine, it just needs to be included in the project description at the start as this has never been mentioned before in the document. It also needs to be added to the data flow document.

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 type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" 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		UK/EU	
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.  Supplier Assurance Framework TEMPLATE		 Supplier Assurance Framework - CardM	
Will the storage be controlled by another party (not the supplier) such as a product/ platform supplier ie AWS, Google, Microsoft? Provide details.		AWS is a sub processor and stores the personal data for use in staff accounts.	
If the data is stored on the cloud the following assessment must be completed by the supplier  Cloud Assessment.xlsx		CardMedic does not store any patient data.  Worksheet in U Information Governar	
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)			


Commented [DJ(FHNFT9)]: If using AWS which is cloud based this will need completing.

Commented [BS(NANIS10R9)]: Asking to complete again

	Certificate	External Penetration Test undertaken (date)	External Penetration Test Report
Cyber Essentials +/- Cyber Assessment Framework (CAF)	CyberEssentials Cert: 41eebeef-1fb1-4cd1-9ba9-c4c5b09260cd	12 July 2023	Summary available Certified Organisations - lasme
ISO 15489 Records Management	N/A		
ISO 27001 Information Security Standards	N/A		
ISO/IEC 27701:2019 Ext to 27001/27002	N/A		
ISO 27017 Cloud Services	N/A		
ISO 27018 PII in public clouds	N/Aa		
Digital Technology Assessment Criteria for Health and Social Care (DTAC)	See separate DTAC  The Digital Technology Assessr	N/A	N/A
ISO 9001 Quality Management Systems	N/A		
Other, please specify	N/A		
If a supplier is used, are they registered with the ICO. Check the register ⁹ and provide the certificate number.	Yes	No	
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
	Registration reference: zA758949		
If a supplier is used, have they completed the Data Security and Protection Toolkit, search the register here ¹⁰	Yes	No	N/A
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
If yes, complete the following	Organisation code	Status	Date Published
	8KL19	Standards Met	05/04/2023

⁹ <https://ico.org.uk/ESDWebPages/Search>

¹⁰ <https://www.dsptoolkit.nhs.uk/OrganisationSearch>

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?	CardMedic uses Amazon S3 data storage. Amazon S3 encrypts (SSE-S3 server side) all new data uploads to any bucket.						
Will it be on a server protected by firewall and network intrusion detection?	Yes, through AWS infrastructure and monitoring. Amazon Web Services are a secure cloud platform environment, access to the environment is via MFA.						
What technical controls are in place to prevent hacking of the data by unauthorised persons?	Regular external penetration tests are conducted whenever a major feature release takes place or where a change is made that requires testing.						
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?	All Data is Encrypted when it is moved to the cloud. CardMedic data is not moved once stored in S3 on AWS. CardMedic consumes APIs for data capture that are all TLS based interfaces.						
Do you have a business continuity plan for the information?	 CardMedic Business Continuity Plan 230:						
What types of backups are undertaken i.e. full, differential or incremental?	<table border="1" style="width: 100%;"> <thead> <tr> <th>Full</th> <th>Differential</th> <th>Incremental</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> </tbody> </table>	Full	Differential	Incremental	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	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?	All access to data is password controlled, administrators use MFA for accessing admin functions. All users authenticate through AWS Cognito security.				
Is there an ability to audit access to the information? Can the supplier audit our data?	Only approved, role-based administrators have access to staff data held within CardMedic system.				
What other security measures are in place, such as physical security, smartcard, Active Directory, multiple factor authentication?	As mentioned above, administrators use MFA for access.				
Is training available to staff for the new system?	<table border="1" style="width: 100%;"> <thead> <tr> <th>Yes</th> <th>No</th> </tr> </thead> <tbody> <tr> <td style="text-align: center;"><input checked="" type="checkbox"/></td> <td style="text-align: center;"><input type="checkbox"/></td> </tr> </tbody> </table>	Yes	No	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	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?
	<p>No registration data is stored on any device that uses CardMedic.</p> <p>User are required to log on to CardMedic using a username and password.</p>



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?	
	<p>Yes</p> <p><input type="checkbox"/></p> <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>	<p>No</p> <p><input checked="" type="checkbox"/></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?	No.
	What is the statutory reason for this sharing? ie direct care	

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?	Data is being sub-processed and stored by AWS.
	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).	N/A
	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.	Users wishing to withdraw their account can do so by emailing the support desk, a link is provided on their profile settings.
	Are arrangements in place for recognising and responding to requests for access to personal data?	All staff have access to the data held by CardMedic in their profile.


Q25	Describe the data flows	
	Please complete the data flow template below to detail how the data is collected, moved and used?	Registration email will be forward using staff working group emails already available in the

	 New Flow Map UPDATED.xlsm	division they work. Staff can register to use the app.  Copy of Copy of Data Flow map (2).xl
	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 these risk?	

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	
	What is the arrangement between the Trust and the supplier/third party concerned?	 Notts LMNS CardMedic Heads of
	What activities will the supplier/third party carry out i.e. storage, transport, processing of data on their platform	CardMedic will use AWS as a sub processor. AWS will sub process the data and store on their cloud.
Q27	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.	Contracts and Data Sharing Agreements to be agreed between SFH and CardMedic.  CardMedic Data Sharing Agreement

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.	<p>The DPIA will be forwarded to the Information Governance Working Group for wider stakeholder engagement. No wider public engagement is required, as their data isn't being processed.</p> <p>Staff have the freedom to choose is they would like to use CardMedic.</p>
Who else do you need to involve within the Trust? ie Digital Innovations Approval Group (DIAG).	 DIAG Scoping Approval Document
Do you need to ask the data processors (supplier) to assist?	No.
Do you plan to consult information security experts, or any other experts?	No.

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 checked="" 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 type="checkbox"/>
	d) processing is necessary in order to protect the vital interests of the data subject or of another natural person	<input 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 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 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 type="checkbox"/>

Stage 8 – Risk Template

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

Completed by: Siobhan Buxton

Role: ICS

Date completed: 18/01/2024

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)	
Loss of system access due to connection failure or server failure either via NHIS or 3 rd party supplier. Result in the service being disrupted or unavailable. The consequences of this could be reputational damage to the Trust	This app is to support gaps in current interpretation services. If CardMedic is unavailable alternative resources should be accessed to support communication needs CardMedic can be accessed offline.	1	1	1		1	1	1	This is to support current interpretation service. No consequences will occur if there is a loss of system.
If the system is not recorded on the information asset register, the system may not be brought back online in response to a cyber attack	This app is to support gaps in current interpretation services. If CardMedic is unavailable alternative resources should be accessed to support communication needs	1	1	1		1	1	1	This is a pilot and will be monitored regularly by the IAO's.

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)	
Lack of adequate data processing agreements with relevant data processors may lead to unauthorised use of data, resulting in regulatory action	A contract and data processing agreement between Sherwood Forest Hospitals and CardMedic developed. Separate processing agreements where necessary will be in place with additional providers of data to AWS.	1	1	1 1		1	1	1	
 Copy of CARDMEDIC Hazard									



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 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. • 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 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.

<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. There is the option for staff to add additional information, which is not compulsory, but their choice. • 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 have appropriate processes in place to check the accuracy of the data we collect, and we record the source of that data. • 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.
<p>Principle 6 – Appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.</p>	<ul style="list-style-type: none"> • 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. • 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.

	<ul style="list-style-type: none"> • 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. • We ensure that any data processor we use also implements appropriate technical and organisational measures.
<p>Principle 7 – Accountability principle</p>	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> <input type="checkbox"/> adopting and implementing data protection policies (where proportionate). <input type="checkbox"/> taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the entire lifecycle of our processing operations. <input type="checkbox"/> putting written contracts in place with organisations that process personal data on our behalf. <input type="checkbox"/> maintaining documentation of our processing activities. <input type="checkbox"/> implementing appropriate security measures. <input type="checkbox"/> recording and, where necessary, reporting personal data breaches. <input type="checkbox"/> carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests.

- | | |
|--|--|
| | <ul style="list-style-type: none"><input type="checkbox"/> appointed a data protection officer; and<input type="checkbox"/> adhering to relevant codes of conduct and signing up to certification schemes (where possible).<input type="checkbox"/> 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 checked="" type="checkbox"/>
Project has met required legislative compliance and poses no significant risks. No further action required.	<input type="checkbox"/>

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks	
Legislative Compliance:	<p>Article 6(1)(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes.</p> <p>Article 6(1) (b61b) 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.</p>
Summary of Risks	Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management.
Identified risks	
The risk	Mitigation
Loss of system access	If CardMedic is unavailable, other resources will be used. No consequences will occur if there is a loss of system.
Loss of system data	Full system back-up process in place.
Data is accessed inappropriately	individual username and passwords are provided.
Adequate data processing agreements with relevant data processors	In Place.
System not being on the Asset register could delay getting it back online in response to a Cyber-attack,	If CardMedic is unavailable, other resources will be used. This is a pilot and will be monitored regularly by the IAO's.

Step 10 - Recommendations for Action

Summary of recommendations (amend/delete as necessary)		
Recommendations	Recommendations	Agreed deadline for action
Information Asset Administrators to ensure CardMedic is added to the information asset register and data flows are mapped and recorded.	IAO/IAA	07/02/2024  Copy of WandC Asset Register 2020.

Step 11 - Project signoff

	Name	Job Title	Date
Information Asset Owner*	Gemma Boyd	Divisional General Manager	02.02.2024
Data Protection Officer	Jacque Widdowson	Information Governance Manager	28.02.2024
Senior Information Risk Owner	Sally Brook Shanahan	Director of Corporate Affairs	18.03.2024
Caldicott Guardian	David Selwyn	Medical Director	27.03.2024
Chief Digital Information Officer	Paul Moore	Acting Chief Digital Information Officer	07.03.2024
Patient safety¹¹			

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.

¹¹ [DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital](#)