Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

Data Protection Impact Assessment

Title	Ref number
Endobase – Endoscopy Software	

Introduction

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

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

Document Completion

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

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

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

Activity	IAO	Governance
Complete Title Bar and include Ref Number	x	
Complete Project Details and check the Initial Screening Questions	x	x

Complete Stage 1 – Introductory meeting and review Initial Screening Questions and follow up questions to determine if a Stage 2 – DPIA (Full) is to be undertaken	x	x
Initial Screening Questions to be formally written up and Introductory Meeting to be formally recorded	x	x

If a Data Protection Impact Assessment **IS NOT** required		
Activity	**IAO**	**Governance**
Complete Assessment Summary & Recommendations for Action	x	x
Assessment to be passed to Implementer		x
Ensure Sign Off is completed	x	x
Assessment shared with customer if appropriate	x	
Assessment to be kept with project documentation copy to Information Governance	x	

OR

If a Data Protection Impact Assessment **IS** required		
Activity	**IAO/IAA**	**Governance**
When a new system is being implemented and the supplier provides a completed DPIA on a suppliers template, the information will need to be transferred to the Trust's template to ensure there are no omissions	**x**	
Complete Stage 2 – Data Protection Impact Assessment (Full)	**x**	
Complete Stage - 3 Identified Risks and Mitigating Action	**x**	
Complete Stage – 4 Legal Compliance		x
Complete Assessment Summary & Recommendations for Action	x	
Account access management Standard Operating Procedure to be completed prior to the implementation of the project	x	
Closure meeting for final agreement	x	
Ensure Sign Off is completed		x
Assessment shared with customer if appropriate	x	
Assessment to be kept with project documentation copy to Information Governance	x	

This document is intended to be completed by the Trust and external organisations the *Governance* section will be completed by the IG Team with support from the relevant NHIS specialist teams as applicable.

Project Details

Project Title:	**Endobase – Endoscopy Software**

Project Description: Describe in sufficient detail for the proposal to be understood
Endobase is a reporting system used by Endoscopist that generates reports from the procedure performed in the Endoscopy Department. Endobase allows the Trust to remain JAG Accredited by allowing data to be sent to the National Endoscopy Database which is hosted by the Royal College of Physicians. The current version of endobase is compatible with Windows 10. The trust being kept JAG accredited will open education opportunities to our endoscopists and will allow the trust to receive more funding per procedure. JAG Accreditation is the national standards that the service is expected to meet.

Overview of the proposal: What the project aims to achieve
To ensure the service remains JAG accredited and install confidence in the service and continue to receive best practice tariff per procedure. The updated version of Endobase allows the system to update how images are captured on the Endoscopes and to provide a clearer image. The updates also support Windows 10.

Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in DPIA assessment (Include Email Address):	Cally Jarvis, Service Manager – Gastroenterology and Endoscopy, cally.jarvis@nhs.net Dr Stephen Foley stephenfoley@nhs.net Pankaj.Patel@Olympus.com Achal.Patel@Olympus.com

Project Sign Off

	Name	Job Title	Organisation	Date

Information Asset Owner	Rachael Briggs	Divisional General Manager – Medicine	Sherwood Forest Hospitals NHS Foundation Trust	26th July 2021
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	26th July 2021
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	23rd July 2021
Senior Information Risk Owner	Paul Robinson	Chief Financial Officer	Sherwood Forest Hospitals NHS Foundation Trust	27th July 2021
Caldicott Guardian	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	21st October 2021
Chief Clinical Information Officer	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	21st October 2021

Assessment Summary

To be completed by Information Governance

Outcome of Data Protection Impact Assessment:	
1. Project/Implementation is recommended **NOT** to proceed, as significant corporate/customer risks have been identified.	☐

2. Project/Implementation to proceed once identified risks have been mitigated as agreed.	☒
3. Project/Implementation has met required legislative compliance and poses no significant risks. No further action required.	☐

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

Summary:

1. Endobase data flows map to be regularly reviewed
2. Endobase to be added to the Information Asset Register for Medicine Division
3. There is a risk of unauthorised access due to the system being unable to report on users that have accessed individual patient records.
4. Data is held on the Trust's servers and in-patient case notes. However it is not clear what the arrangements are for the deletion of data on the Endobase system once the contract expires in 2026.

Summary of Risks:

Information Asset Management

Not able to capture inappropriate access to data

Data is held on the Trust's servers and in-patient case notes. However it is not clear what the arrangements are for the deletion of data on the Endobase system once the contract expires in 2026.

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	**Recommendation Owner:**	**Agreed Deadline for action:**
Regularly review and update as necessary the data flows in Endoscopy	IAA	31st December 2021
Update the Medicine Division Information Asset Register	IAA	31st December 2021
Annual review of the contract to ensure that once the functionality to audit access is provided that the DPIA is updated to reflect this.	IAO	31st July 2022
Arrangements for deleting the data held in Endobase need to be included in the contract	IAO	31st July 2022
Not able to capture inappropriate access to data – implement Standard Operating Procedure for access controls. Information Governance to provide this	IAO	31st August 2021

Stage 1 – Initial Screening Questions

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

Q	Screening question	Y/N	Justification for response
1	Will the project involve the collection of information about individuals?	Y	When the patient is given a TCI (to come in) date the demographics are fed through from CareFlow (live feed)
2	Will the project compel individuals to provide information about themselves?	N	
3	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	N	
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	N	
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	Yes we check the demographics with the patient, CareFlow and also the NHS Spine
6	Are there security arrangements in place while the information is held?	Y	Endobase data is stored on the Trust's servers maintained by NHIS
7	Does the project involve using new technology to the organisation?	N	
8	Will the project result in you making decisions or taking action against individuals in ways which could have a significant impact on them?	N	
If you have answered "Yes" to any of the questions numbered 1-8 please proceed and complete stage 2.			
9	Is a Patient Safety Review required?	Y	The patient safety case was approved June 2019
10	Is a Quality Impact/Technical Security Review required?	Y	NHIS have reviewed the July 2021 responses from Olympus. No issues identified

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

Stage 2 – Data Protection Impact Assessment

2.1	What is the change					
	New purpose?	☐	Revised/changed?	☒	Other?	☐
	If Other please specify.					

2.2.1	What data will be processed?					
	Personal Data:					
	Forename	☒	Surname	☒	Age	☒
	DOB	☒	Gender	☒	Address	☒
	Post Code	☒	NHS No	☒	Hospital No	☒
	Other unique identifier (please specify)					
	Sensitive Personal Data (special categories):					
	Children					☐
	Vulnerable groups					☐
	Racial or ethnic origin					☐
	Political opinion					☐
	Religious Belief					☐
	Trade Union Membership					☐
	Physical or mental health or condition					☒
	Sexual Health					☐
	Criminal offence data					☐
	Other data (please specify)					

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

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	Data is used to produce reports based on the findings in a patient's procedure. Data is also queried to audit areas of Endoscopy to ensure the department is still meeting standards.

2.3.1	How will you collect, use, store and delete data?
	Data is collected as a patient is booked for a procedure by the administration team on CareFlow EPR, which is then fed through to Endobase via HL7. Further data is collected during procedures by the Endoscopists with images and the details of the procedure are entered into a report on Endobase. Comfort scores are also entered into Endobase by the Clinical Audit Assistant after the procedure has taken place. Data is used to create reports for individual procedures. Data is also used to create reports for audits on procedures and Endoscopists. Data is stored on Trust servers. Data is deleted in accordance with the Trust's Retention and Destruction Policy and Records Management Code of Practice.
2.3.2	What is the source of the data? (i.e. from data subject, system or other third party)
	Data Subject and CareFlow EPR
2.3.3	How much data will you be collecting and using?
	80 individuals per day offering a 7-day service, the minimum data is collected in order to undertake the procedure
2.3.4	How often? (for example monthly, weekly)
	Daily

2.3.5	How long will you keep it?  NHSX_Records_Management_Code_of_Prac
	Data will be held and destroyed as per the trust wide Retention and Destruction Policy and Records Management Code of Practice. Arrangements for deleting the data held in Endobase need to be included in the contract
2.3.6	Where will the data be stored? i.e. CareFlow EPR, Shared Drive, offsite storage
	The data will be held on Trust servers and accessed via Endobase. 3 copies of the report are printed from Endobase. One for the patient, one for the GP and one for the case notes
2.3.7	How many individuals are affected?
	80 individuals per day offering a 7-day service
2.3.8	What geographical area does it cover?
	Nottinghamshire, Derbyshire, Lincolnshire

2.4	Who are the Organisations involved in processing (sharing) the data?	
	Organisations Name	Data Controller or Data Processor *The **Data Controller** is a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed.* *The **Data Processor**, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller.*
	Sherwood Forest Hospitals NHS Foundation Trust	Data Controller
	KeyMed (Medical & Industrial Equipment) Ltd (Olympus)	Data Processor

	Sirona	Data Processor – an external company we are using for the insourcing at the weekend to expand the capacity of the service to see more patients

2.5	If we have identified a supplier in 2.4, the following questions for 2.5 and 2.6 will need to be answered by the supplier and the Trust	
	Y/N	**If yes the third party will need to complete the following assessment. This will need to be provided in addition to the completion of this proforma. An example of a completed assessment is also provided below**  NHIS - Supplier Assurance Framework  Supplier Assurance Framework - Example
	Y	Read only access will be provided to Olympus when on-site and have 3rd party access via NHIS to update the software on the Trust's servers remotely.  Endobase 2021 Submission.xlsx
2.5.1	Please describe access and controls in place Account access management Standard Operating Procedure to be completed prior to the implementation of the project	
	NHIS give access to the file path with names provided by Endoscopy There are super users in Endoscopy that then create a username and password to access the system. Endoscopy staff remove access once the individual leaves the department A Standard Operating Procedure is to be developed, for account management and access. This needs to be in place as soon as and no later than 30th August.	
2.5.2	Please provide a copy of the contract in place	
	The Trust also has a maintenance contract in place with Olympus for the medical equipment.	

	INFOCUS T&Cs UK - Complete Plus - Appe INFOCUS CPQ Multi-Year Sherwood INFOCUS_Brochure.pdf			
2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?			
	Data is held on the Trust's servers and in-patient case notes. However it is not clear what the arrangements are for the deletion of data on the Endobase system once the contract expires in 2026. Raised as a risk			
2.5.4	Is the supplier registered with the ICO? Please check the register		Yes	No
			X Z707164X	
2.5.5	Has the supplier received ICO Enforcement? Please check the register		Yes	No
				x
2.5.6	Has the supplier received ICO Decision Notice? Please check the register		Yes	No
				x
2.5.7	Has the supplier received an ICO Audit? Please check the register		Yes	No
				x
2.5.8	Has the supplier completed a Data Security and Protection Toolkit, please check the register and provide the following details	Completed: Yes/No	Date submitted	Standard Met/Not Met
		Yes	09/12/2020	Standards Met
2.5.9	Can the supplier demonstrate compliance with any of the following standards? If YES please provide further information e.g. date achieved and a copy of the certificates			
		Yes	No	
	Cyber Essentials Plus		No, we have CE only	

	ISO 15489 Records Management		No
	ISO 27001 Information Security Standards		No
	ISO 9001 Quality Management Systems	Yes	

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

2.6	Will this information be shared outside the organisations listed above?	
	Y/N	if answered **Yes** please describe organisation/s and geographic location
	Y	Information of Endoscopists, procedures and procedure times will be sent to the National Endoscopy Database, hosted by the Royal College of Physicians JAG Office Accreditation Unit Care Quality Improvement Department Royal College of Physicians 11 St Andrews Place Regent's Park London NW1 4LE GP practice will be sent a paper copy

2.7	Does the work involve employing contractors external to the Organisation?	
	Y/N	If **Yes**, provide a copy of the confidentiality agreement or contract?

	Y	Sirona, an external company we are using for the insourcing at the weekend to expand the capacity of the service to see more patients. Sirona employees will have access to Endobase whilst onsite.				
2.8	Has a data flow mapping exercise been undertaken?					
	Y/N	If **Yes**, please provide a copy here. If No, please explain why				
	Have the information flows and assets that are identified within this DPIA been added to your departmental information flow map and asset register? If No, please explain why					
	Y	Copy of ENDOBASE Flow Map.xlsm				
2.9	What format is the data?					
	Electronic	☒	Paper	☒	Other (Please describe)	3 copies of the report are printed from Endobase. One for the patient, one for the GP and one for the case notes

2.10	Is there an ability to audit access to the information?	
	Y/N	Please describe if answered **Yes.** If **NO** what contingencies are in place to prevent misuse?
	N	Endobase Development Team are working on functionality to enable to audit who has accessed individual patient records in the system. This is not currently available.

2.11	Does the system involve new links with personal data held in other systems or have existing links been significantly changed?	
	Y/N	Please describe if answered **Yes**
	N	The data submission from Endobase to the National Endoscopy Database (NED) is a deployed as a module of

		the Endobase system I believe, so provided and supported by Olympus. https://www.thejag.org.uk/National-Endoscopy-Database will provide a brief description (s2.11),

2.12	How will the information be kept up to date and checked for accuracy and completeness? (data quality) How will you ensure data minimisation?	
	Data is regularly audited; any anomalies in the data shall be reported and fed back to the Endoscopy team on how data is being entered to ensure data is being entered correctly. All Endoscopists should follow the writing good endoscopy reports section of the Endoscopy Operational Policy.	
2.13	Who will have access to the information? (list individuals or staff groups)	
	Gastroenterology Consultants Urology Consultants Bronchoscopists The Gastroenterology and Endoscopy Administration Teams Sirona Medical Limited (Endoscopy Insourcing Company) – confidentially agreements for access to the system and a Windows Account will be provided.	
2.14.1	What security measures have been implemented to secure access?	
	Active Directory (Window's username and password)	☒
	Username and password	☒
	Smartcard	☐
	Key locked filing cabinet/room	☐
	Hard/soft Token (VPN) Access	☐
	Restricted Access to Network Files (shared drive)	☒

	Has information been anonymised?	☐
	Has information been pseudonymised?	☐
	Is information fully identifiable?	☒
	Other (provide detail below)	☐
2.14.2	What physical security measures have been implemented to secure access? ie swipe cards, digilock	
	Access to the information is via Endobase using a username and password which is created by the administration staff in Endoscopy. NHIS create the Windows accounts. Case notes are stored in a secure area in the Endoscopy suite	
2.15	Will the data be stored on Trust servers	
	Yes	No
	✓ However, data will be sent to the National Endoscopy Database in accordance with JAG standards. The data is transmitted via HL7 and encrypted both in transit and at rest. HL7 - Health Level Seven® International (HL7®) is the global authority on standards for interoperability of health technology and is the global industry standard for passing healthcare data between systems. 3 copies of the report are printed from Endobase. One for the patient, one for the GP and one for the case notes.	

2.16	Please state by which method the information will be transferred?			
	Email (not NHS.net)	☐	NHS.net	☐

	Website Access (internet or intranet)	☐	Wireless Network (Wi-Fi)	☐
	Secure Courier	☐	Staff delivered by hand	☐
	Post (internal)	☐	Post (external)	☒
	Telephone	☐	SMS	☐
	Other	☒	please specify below	☐
	3 copies of the report are printed from Endobase. One for the patient, one for the GP and one for the case notes.			

2.17	Are disaster recovery and business contingency plans in place for the information? What types of backups are undertaken i.e. full, differential or incremental?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	We revert back to paper reports in the event Endobase is unavailable. We have a business continuity plan in place.

2.18	Has staff training been proposed or undertaken and did this include confidentiality and security topics areas?	
	Y/N	Please describe if answered **Yes**
	Y	All members of staff receive mandatory information governance training annually. Additional training on how to access and use the Endobase system is provided prior to staff accessing the system.

2.19	Will reports be produced?

	Will reports contain personal/sensitive personal or business confidential information?	Yes
	Who will be able to run reports?	Users with specific access
	Who will receive the reports and will they be published?	A paper copy of the patient's endoscopy report is posted to the GP

2.20	If this new/revised function should stop, are there plans in place for how the information will be **retained / archived/ transferred or disposed of?**	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	Deep archive servers transfer to another organisation process.
2.21	Is consent required for processing of personal data?	
	Y/N	Please describe if answered **Yes**
	N	
		If **No**, list the reason for not gaining consent e.g. relying on an existing agreement, consent is implied, the project has s251 approval or other legal basis?
	N	Part of our statutory duties to provide healthcare under GDPR 6(1)(e) public interest or public duty
2.22	Will individuals be informed about the proposed uses and share of their personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The service uses Endobase software package to record the finding of the endoscopy procedure and produce a final report which is shared with the Patient, their GP and printed for a copy to be retained on their paper patient record file.

		The Trust's privacy notice is here https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/ KeyMed's privacy notice is here: https://www.olympus.co.uk/company/en/privacy-notice/
2.23	Is there a process in place to remove personal data if data subject refuses/removes consent	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The Trust has access to do so but has not been asked to undertake it.
2.24	How much control will they have? Would they expect you to use their data in this way?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	This system is used to record the outcome of an endoscopy and is direct care. Patients consent to the procedure.
2.25	Are arrangements in place for recognising and responding to requests for access to personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The Trust has an established process for responding to subject access requests Sherwood Forest Hospitals (sfh-tr.nhs.uk)
2.26	Who are the Information Asset Owner(s) and Administrator(s)?	
	IAO	Rachael Briggs, Divisional General Manager
	IAA	Cally Jarvis, Service Manager – Gastroenterology and Endoscopy
	System Administrators	Emma White, Business Support Officer, Natalie Holt, Endoscopy Clerical Officer, Josh Bailey, Endoscopy

		Clerical Officer and Dr Foley, Consultant Gastroenterology and Endoscopy Service Lead
2.27	How is the data secured in transit and at rest? Eg encryption, port control number	
	Data is stored in the Endobase system on Trust servers. However data from the Endobase system is transferred to the national endoscopy database via HL7Further information on the JAG on GI Endoscopy is available here	
2.28	Has the impact to other NHIS systems/processes been considered and appropriate SBU's consulted and in particular technical security?	
	Y/N	Please describe if answered **Yes.** Please state what checks were undertaken if response is answered **No.**
	Y	A patient safety test was undertaken on the system and the devices and approved in June 2019.
2.29	Are there any current issues of public concern that you should factor in?	
	Y/N	Please describe if answered **Yes.**
	N	
2.30	What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?	
	To ensure the service remains JAG accredited and install confidence in our service. The Endobase upgrade updated how images are captured on the endoscopes and provide a clearer image. Joint Advisory Group (JAG) - JAG works across three main areas: endoscopy training, accreditation of endoscopy services and accreditation of screening endoscopists. JAG also spearheads quality improvement (QI) initiatives to drive up standards of care for patients.	
2.31	Consider how to consult with relevant stakeholders: • Describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. • Who else do you need to involve within your organisation? • Do you need to ask your processors to assist?	
	The Information Governance Working Group and Committee will review the data protection impact assessment and any comments/actions taken	

	forward. NHIS have reviewed in relation to patient safety and technical security. KeyMed have provided information to support the completion of this assessment. Forward to Dr Foley who is leading on the project.

2.32	What is your lawful basis for processing? (please see Appendix 10 Information Sharing Protocol for further information). **Consent is usually the last basis to rely on** **Legal basis: patients** **Personal data i.e. name, address** 6(1)(a) the patient has given consent 6(1)(c) necessary for legal obligations 6(1)(e) public interest or public duty 6(3) the above supported by Member State law (UK legislation as applicable to circumstances) **Sensitive personal data (special category)** 9(2)(a) the patient has given explicit consent 9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc.) 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity). 9(2)(i) allows processing for "ensuring high standards of quality and safety of health care." – which would cover research, audit, service improvement and addressing public health/inequalities. 9(2)(j) (together with Article 89 and relevant recitals) relates to archiving, statistical analysis and research. **Legal basis: staff** – please review Appendix 10 Information Sharing Protocol for further information).
	The Trust's lawful basis for processing personal and special categories of personal data are:

	1. Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. 2. Article 9(2)(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject 3. Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
2.33	What information will you give individuals about the processing? (This information will be added to the Trust's Patient Privacy Notice and Staff Privacy Notice by the Information Governance Team)
	This document will be published once finalised. There were posters in the department, but we had to remove all posters due to Covid-19.

2.34	What measures do you take to ensure processors comply?
	We have a contract in place with the supplier.
2.35	How will you prevent function creep? Manage lifecycle of system/process
	KeyMed will only ever process the Trust's data as per explicit agreement with the Trust The Trust and KeyMed have a contract in place where roles and responsibilities are defined.

Stage - 3 Risk Template

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

Completed by Gina Robinson	Role: Information Security Officer	Date completed: 22nd July 2021

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
All data flows are not recorded in the Medicine division	Annual programme of work with the Information Asset Owners to seek assurance around the assets used in the Trust	3	2	6	Endobase data flow maps to be regularly reviewed	1	1	**1**	Endobase data flows map to be regularly reviewed
Endobase to be added to the Information Asset Register for Medicine Division	Annual programme of work with the Information Asset Owners to seek assurance around the assets used in the Trust	3	2	6	Assets need to be added to the Information Asset Register	1	1	**1**	Assets need to be added to the Information Asset Register
There is a risk of unauthorised access due to the system being unable to report on users that have accessed individual patient records.	Annual programme of work with the Information Asset Owners to seek assurance around the assets used in the Trust	3	3	9	Staff to ensure that annual Data Security training is undertaken. Account Management and access procedure to be completed. There is no assurance in place at the moment as there are currently no controls in place.	2	1	**2**	Improved audit functionality by the supplier

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Data is held on the Trust's servers and in-patient case notes. However it is not clear what the arrangements are for the deletion of data on the Endobase system once the contract expires in 2026	The Trust and the supplier have a contract in place	2	2	4	Retention and destruction arrangements will need to be defined and included in the contract	2	1	**2**	Review of the contract

Risk Scoring Matrix.pdf

Stage – 4 Legal Compliance

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

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

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

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