Healthier Communities, Outstanding Care

Sherwood Forest Hospitals NHS Foundation Trust

Data Protection Impact Assessment

Title	Ref number
CFH Docmail Limited and Central Aspects of Pain in Rheumatoid Arthritis (CAP-RA)	

Introduction

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

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

Document Completion

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

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

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

Activity	IAO	Governance
Complete Title Bar and include Ref Number	x	

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

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

OR

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

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

Project Details

Project Title:	CFH Docmail Limited and Central Aspects of Pain in Rheumatoid Arthritis (CAP-RA)

Project Description: Describe in sufficient detail for the proposal to be understood
Improving Pain Outcomes in Rheumatoid Arthritis; Detecting the Contribution of Central Pain Mechanisms.

Overview of the proposal: What the project aims to achieve
Objectives: 1. Optimise and measure the psychometric properties of Central Aspects of Pain in Rheumatoid Arthritis (CAP-RA) in people with Rheumatoid Arthritis. 2. Measure the ability of Central Aspects of Pain in Rheumatoid Arthritis (CAP-RA) to identify people with active Rheumatoid Arthritis destined to have poor fatigue outcome despite therapy. Secondary Objectives 1. Investigate factors associated with worse Rheumatoid Arthritis pain 2. Compare Central Aspects of Pain in Rheumatoid Arthritis (CAP-RA)'s persistent pain performance to other pain outcome predictors 3. Derive Central Aspects of Pain in Rheumatoid Arthritis (CAP-RA) scoring recommendations for stratification in clinical trials and clinical practice, 4. Examine the association between central pain sensitization and fatigue. 5. Examine 12-week course of pain and fatigue in Rheumatoid Arthritis Methods: 250 people with Rheumatoid Arthritis will complete the Central Aspects of Pain in Rheumatoid Arthritis (CAP-RA) questionnaire, answer questions about pain, fatigue and other areas of health, and undergo other tests and scans to measure pain, fatigue, inflammation, and central sensitization. We will use their data to determine how well Central Aspects of Pain in Rheumatoid Arthritis (CAP-RA) works in people with painful Rheumatoid Arthritis and measure the extent to which pain and fatigue are related to central sensitization. We will also see if Central Aspects of Pain in Rheumatoid Arthritis (CAP-RA) can be used to predict who will still have unacceptable pain, despite treatment. Impact: We anticipate that Central Aspects of Pain in Rheumatoid Arthritis (CAP-RA) will identify which people can benefit from treatments over and above those treating inflammation. We will use findings from this study to develop new ways of treating people with Rheumatoid Arthritis in order to improve their pain and fatigue. Mailings are created through CFH Docmail Limited's https: web portal and will only use Title, Name and Address for the mailshot

Implementing Organisation:	Sherwood Forest Hospitals NHS Foundation Trust

Staff involved in DPIA assessment (Include Email Address):	Terri-Ann Sewell, Research Operations Manager and Donna Sowter, Research Support Facilitator / Information Manager

Project Sign Off

	Name	Job Title	Organisation	Date
Information Asset Owner	Alison Steel	Head of Research and Innovation	Sherwood Forest Hospitals NHS Foundation Trust	18th August 2022
Data Protection Officer	Jacquie Widdowson	Information Governance Manager	Sherwood Forest Hospitals NHS Foundation Trust	3rd August 2022
Information Governance	Gina Robinson	Information Security Officer	Sherwood Forest Hospitals NHS Foundation Trust	27th July 2022
Senior Information Risk Owner	Shirley Higginbotham	Director of Corporate Affairs	Sherwood Forest Hospitals NHS Foundation Trust	8th August 2022
Caldicott Guardian	David Selwyn	Medical Director	Sherwood Forest Hospitals NHS Foundation Trust	11th September 2022

Chief Digital Information Officer	Richard Walker	Chief Digital Information Officer	Sherwood Forest Hospitals NHS Foundation Trust	**13th September 2022**

Assessment Summary

To be completed by Information Governance

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

Summary of Data Protection Impact Assessment; including legislative compliance and identified risks:
Summary: Legislative Compliance: Article 6(1)(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. Article 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity) Article 9(2)(i) allows processing for "ensuring high standards of quality and safety of health care." – which would cover research, audit, service improvement and addressing public health/inequalities **Summary of Risks**: Cyber security, loss of data, inappropriate access to data, inability to access data and Information Asset Management. **Risks**

1. Loss of system access - Full system back-up process in place
2. Loss of system data - Full system back-up process in place
3. Leavers' access not removed - research team notified of leavers by HR. Changes to user roles reviewed monthly via a Trust e-form report
4. Business continuity plans in each area, users have business continuity plans for their areas/departments. Not having these could lead to access to data problems or service delivery problems.
5. CFH Docmail Limited will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO
6. Data is accessed inappropriately – individual username and passwords are provided. Once a password is set it remains until the user changes it. The system requires a strong password

Recommendations for Action

Summary of Identified Recommendations:		
Recommendations:	**Recommendation Owner:**	**Agreed Deadline for action:**
Information Asset Administrators to ensure CFH Docmail Limited is added to the information asset register and data flows are mapped and recorded	IAA	31st August 2022
Ensure business continuity plans are in place , the department will revert back to paper based system should there be any issues.	IAA	31st August 2022
Account management Standard Operating Procedure generated and implemented	IAA	31st August 2022
Routine audit to take place, audit cycle to be indentified		31st August 2022
Users to regularly change their password in line with the Trust's Password Management Procedure. Password change will be prompted by the DOCMAIL system		31st August 2022

Stage 1 – Initial Screening Questions

Answering "**Yes**" to a screening questions below represents a potential IG risk factor that may have to be further analysed to ensure those risks are identified, assessed

and fully mitigated. The decision to undertake a full DPIA will be undertaken on a case-by-case basis by IG.

Q	Screening question	Y/N	Justification for response
1	Will the project involve the collection of information about individuals?	Y	Title, Name and Address required to be added to mailshot
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?	Y	Title, Name and Address
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?	Y	In order to screen and gauge an interest in participating in a research trial
5	Are there processes in place to ensure data is relevant, accurate and up-to-date?	Y	Excel spreadsheet populated by the research team. Demographics are not a direct feed from CareFlow EPR
6	Are there security arrangements in place while the information is held?	Y	CFH Docmail Limited hold the following certifications: • SCCI0129 – Clinical Risk Management (Docmail) • ISO 9001:2015 Quality Management System • ISO 14001:2015 Environmental Management System • ISO 27001:2013 Information Security Management System • NHS Digital Data Security and Protection Toolkit • Cyber Essentials • Cyber Essentials Plus • Registered with the Information Commissioner's Office (ICO).
7	Does the project involve using new technology to the organisation?	N	

Q	Screening question	Y/N	Justification for response
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? DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital	N	SCCI0129 – Clinical Risk Management (Docmail) accreditation. 14th June 2022 – NHIS have confirmed that a patient safety case is not required
10	Is a Quality Impact/Technical Security Review required?	N	The supplier is ISO:27001 and Cyber Essentials + certified. Due to these accreditations a further review using the Trust's supplier assurance framework is not required.

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)		GP			
	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					
	During implementation CFH Docmail Limited's IT team will support NHIS to set up a secure FTP connection from their approved HSCN server. All data coming into CFH Docmail Limited is automatically virus checked and all data transferred is made in accordance with ISO 27001 Information Security Management certification.					

2.3	Is the data required to perform the specified task?	
	Y/N	Please justify response **Yes or No**
	Y	Title, Name and Address require in order to post mailshot
2.3.1	How will you collect, use, store and delete data?	
	Data will be entered onto a spreadsheet and uploaded to the DOCMAIL system. The spreadsheet will be saved on a secure drive electronically for the duration of the trial and retention period (usually 15 years for Research)	
2.3.2	What is the source of the data? (i.e. from data subject, system or other third party)	
	Data subject, hospital applications/notes	
2.3.3	How much data will you be collecting and using?	
	Title, Name and Address, 300+ patients	
2.3.4	How often? (for example, monthly, weekly)	
	Weekly	
2.3.5	How long will you keep it? https://www.sfh-tr.nhs.uk/media/12002/isp-101-records-management-code-of-practice-2021.pdf	
	All mailing data is deleted once the retention period has been met. CFH Docmail Limited will retain mailing data for 28 days from the date our order was	

	dispatched. In the event that "returns management services" are selected against an order, the name and address will be held for 60 days in order to process any returned mail items.
2.3.6	Where will the data be stored? i.e., CareFlow, Shared Drive, offsite storage
	All mailing data is stored in a secure (ISO:27001 certified) storage location within CFH Docmail Limited's infrastructure.
2.3.7	How many individuals are affected?
	The number of affected individuals is around 300+ patients
2.3.8	What geographical area does it cover?
	North Nottinghamshire and Derbyshire patients

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
	CFH Docmail Limited CFH Docmail Limited (Reg. Co. No.: 01716891) Main postal address: CFH Docmail Limited, St Peters Park, Wells Road, Westfield, Radstock, BA3 3UP Main telephone number: 01761 416311 Alternative postal address: CFH Docmail Limited, Starlaw Business Park, Livingston, EH54 8SF	Data Processor

	Alternative telephone number: 01506 462468 By email: data.protection@cfh.com	

2.5	If we have identified a supplier in 2.4, the following questions for 2.5 will need to be answered by the **supplier and the Trust**	
	Y/N	**If yes the third party will need to complete the following assessment. This will need to be provided in addition to the completion of this proforma. An example of a completed assessment is also provided below**  NHIS - Supplier Assurance Framework  Supplier Assurance Framework - Example  Cloud Assessment.xlsx
		The supplier is ISO:27001 and Cyber Essentials Plus certified. Due to these accreditations a further review using the Trust's supplier assurance framework is not required.
2.5.1	Please describe access and controls in place Account access management Standard Operating Procedure to be completed prior to the implementation of the project https://www.sfh-tr.nhs.uk/media/12007/ig-012-account-management-and-access-policy-2021.pdf  Account Management & Acces	
	Completed above. CFH Docmail Limited retail a log of activity and review on a quarterly basis. The Trust administrators will delete users once they no longer require access. Accounts are classed as inactive and liable for deletion after two years from the last login, transaction and mailing. A warning email is sent to the account owner 7 days prior to account deletion. Note this applies to accounts, not users.	
2.5.2	Please provide a copy of the contract in place	

	 UoN NCA Interventional Studi			
2.5.3	Have arrangements for retention and destruction been included in the contract when the service/contract expires?			
	All mailing data is deleted once the retention period has been met. CFH Docmail Limited will retain mailing data for 28 days from the date our order was dispatched. In the event that "returns management services" are selected against an order, the name and address will be held for 60 days in order to process any returned mail items.			
2.5.4	Is the supplier registered with the ICO? Please check the register		Yes	No
			Z5722574	
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. 8HN70	8th March 2022	Standards Exceeded
2.5.9	Can the supplier demonstrate compliance with any of the following standards? If YES please provide further information e.g. date achieved and a copy of the certificates			
		Yes	No	
	Cyber Essentials Plus	X		

		CFH Docmail Ltd (including PRINT.UK.C	
	ISO 15489 Records Management		x
	ISO 27001 Information Security Standards	X CFH Docmail Ltd (including PRINT.UK.C	
	ISO 9001 Quality Management Systems	X CFH Docmail Ltd ISO 9001_2015 Certificate	

2.5.10	Is the data held outside of the UK ie Europe, USA, Ireland? If yes please include the country	
	Yes	No
		Radstock and Livingston, England
	If yes we need to seek assurance that the data will continue to flow post Brexit 31.12.2020, provide further detail below from the supplier	
	Not applicable	
2.6	Will this information be shared outside the organisations listed above?	
	Y/N	if answered **Yes** please describe organisation/s and geographic location
	N	

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

2.8	Has a data flow mapping exercise been undertaken?					
	Y/N	If **Yes**, please provide a copy here. If No, please explain why				
	Have the information flows and assets that are identified within this DPIA been added to your departmental information flow map and asset register? If No, please explain why					
	The Trust will need to map the flow of data for this service. Added as a recommendation to the DPIA.					
2.9	What format is the data?					
	Electronic	☒	Paper	☐	Other (Please describe)	Click here to enter text.

2.10	Is there an ability to audit access to the information?	
	Y/N	Please describe if answered **Yes.** If **NO** what contingencies are in place to prevent misuse?
	Y	Monitoring through CFH Docmail Limited SIEM software and access is monitored and audited

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	

2.12	How will the information be kept up to date and checked for accuracy and completeness? (data quality) How will you ensure data minimisation?
	The supplier requires the following information only Title First name Surname Address 1 Address 2 Address 3 Address 4 GP Code
2.13	Who will have access to the information? (list individuals or staff groups)
	Research and Rheumatology Team, DOCMAIL
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			
	Physical access to the server rooms and remote access to the servers is restricted to those who require access to perform their duties.			
2.15	Will the data be stored on Trust servers			
	Yes	No		
		x		
2.16	Please state by which method the information will be transferred?			
	Email (not NHS.net)	☐	NHS.net	☐
	Website Access (internet or intranet)	☒	Wireless Network (Wi-Fi)	☐
	Secure Courier	☐	Staff delivered by hand	☐

	Post (internal)	☐	Post (external)	☐
	Telephone	☐	SMS	☐
	Other	☐	please specify below	☐

2.17	Are disaster recovery and business contingency plans in place for the information? What types of backups are undertaken i.e. full, differential or incremental?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	In the Trust we have a business continuity plan if the service was unavailable. The department would default back to the current practice and access the information manually. The supplier is ISO27001 and Cyber Essentials + compliant

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**
		Relevant Trust employees will receive training on how to use the system. The following guide has been produced to support this training. Introduction to CFH Docmail Ltd for King l SOP-AR035 Docmail.docx

2.19	Will reports be produced?	
	Will reports contain personal/sensitive personal or business confidential information?	No
	Who will be able to run reports?	All users with access to the

		system at the Trust
	Who will receive the reports and will they be published?	The reports are automatically sent to specified e-mail accounts or requested on an adhoc basis from the supplier

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.**
		The report is being filed in the patient's case notes and will follow the Trusts retention and destruction arrangements. Once a mailing has been submitted, posted and despatched data is held for 14 days, if a mailing has not been submitted but is in draft form only it is held for 28 days. In both cases files automatically delete once the retention period ends.

2.21	Is consent required for processing of personal data?	
	Y/N	Please describe if answered **Yes**
	N	
		If **No**, list the reason for not gaining consent e.g. relying on an existing agreement, consent is implied, the project has s251 approval or other legal basis?
		Part of our statutory duties under GDPR 6(1)(e) public interest or public duty, and Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

2.22	Will individuals be informed about the proposed uses and share of their personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
		The Trust's privacy notice is here https://www.sfh-tr.nhs.uk/for-patients-visitors/your-medical-record/ Supplier privacy notice is available here https://www.cfh.com/policies/CFH-Privacy-Policy-2021.pdf Invite letter sent to patients Order_39124420_Proof_Second_Class_1.pd
2.23	Is there a process in place to remove personal data if data subject refuses/removes consent	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	N	Part of our statutory duties under GDPR 6(1)(e) public interest or public duty, and Article 9(2)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
2.24	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	Letters will be sent on behalf of the patients usual care team to invite them to participate in Research CAP-RA Participant invitation letter final v

2.25	Are arrangements in place for recognising and responding to requests for access to personal data?	
	Y/N	Please describe if answered **Yes.** Please state why not if response is **No.**
	Y	The Trust has a policy and procedure for responding to subject access requests. Further information for patients on how to access their records is here: Sherwood Forest Hospitals (sfh-tr.nhs.uk)
2.26	Who are the Information Asset Owner(s) and Administrator(s)?	
	IAO	Alison Steel, Head of Research and Innovation
	IAA	Terri-Ann Sewell, Research Nurse / Donna Sowter, Information Manager, Research
	System Administrators	Philip Buckley, Research Practitioner /, Bonnie Millar, Musculoskeletal Project Manager, University of Nottingham From CFH Docmail Limited no one administers accounts, other than to provide product support. CFH Docmail Limited operate a zero-privilege system where none of their staff have access to client (Trust) data without a specific requirement to do so.
2.27	How is the data secured in transit and at rest? Eg encryption, port control number	
	During implementation CFH Docmail Ltd.'s IT team will support NHIS to set up a secure FTP connection from their approved HSCN/N3 server. All data coming into CFH Docmail Limited is automatically virus checked and all data transfer is made in accordance with ISO 27001 Information Security Management certification.	
2.28	Has the impact to other NHIS systems/processes been considered and appropriate SBU's consulted and in particular technical security?	
	Y/N	Please describe if answered **Yes.** Please state what checks were undertaken if response is answered **No.**

		DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems - NHS Digital
	Y	SCCI0129 – Clinical Risk Management (Docmail) accreditation. 14th June 2022 – NHIS have confirmed that a patient safety case is not required
2.29	Are there any current issues of public concern that you should factor in?	
	Y/N	Please describe if answered **Yes.**
	N	
2.30	What do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?	
	To improve the management of contacting patients eligible for the Central Aspects of Pain in Rheumatoid Arthritis (CAP-RA) study	
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?	
	presented this document to the Information Governance working group for consultation.	

2.32	What is your lawful basis for processing? (please see Appendix 10 Information Sharing Protocol for further information). **Consent is usually the last basis to rely on** **Legal basis: patients** **Personal data i.e. name, address** 6(1)(a) the patient has given consent 6(1)(c) necessary for legal obligations 6(1)(e) public interest or public duty

	6(3) the above supported by Member State law (UK legislation as applicable to circumstances) **Sensitive personal data (special category)** 9(2)(a) the patient has given explicit consent 9(2)(c) processing for 'vital interests' (safety, safeguarding, public safety, etc.) 9(2)(h) allows processing for the provision of healthcare (direct care) or the management of healthcare systems (invoice validation, commissioner reporting, quality audits – essentially, mandated activity). 9(2)(i) allows processing for "ensuring high standards of quality and safety of health care." – which would cover research, audit, service improvement and addressing public health/inequalities. 9(2)(j) (together with Article 89 and relevant recitals) relates to archiving, statistical analysis and research. **Legal basis: staff** – please review Appendix 10 Information Sharing Protocol for further information).
	The Trust's lawful basis for processing personal and special categories of personal data are: 1. 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. Supplier 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)(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.
2.33	What information will you give individuals about the processing? (This information will be added to the Trust's Patient Privacy Notice and Staff Privacy Notice by the Information Governance Team)
	This DPIA will be published once finalised. The Trust's privacy notice has been updated with the following information: This project aims to understand how information about how risk is communicated before an operation. This understanding will help us to make recommendations about how to improve communication before an operation. Improved communication will help surgeons and patients to decide about the operation in a more informed way. Our project involves three work packages: 1. Audio-recording consultations between patients and surgeons when they discuss the possibility of knee replacement. 2. Asking patients and surgeons how they would like to discuss risks, benefits and other aspects of recovery and outcomes. 3. Using these findings to help us understand how best to design a tool to help patients and professionals make decisions about knee replacement. The project will provide the information that is needed to design a future information resource that is ready for testing and use in the NHS. The research will provide benefits to: • Patients: they will be well informed about their operation, so that expectations match current evidence and their choice to have an operation is based on this. • Surgeons and other health professionals: they will have guidance about areas to discuss in consultations to ensure that consent is fully informed. • NHS: the NHS can have confidence that patients and professionals work together to make the most informed choices possible. The NHS has prioritised informed choice and decision making, and this study reflects this.

2.34	What measures do you take to ensure processors comply?
	CFH Docmail Limited is not aware of any sub processors involved in this project, for which it is responsible for ensuring compliance. The Trust and CFH Docmail Limited have a contract in place and this will be reviewed on a regular basis.
2.35	How will you prevent function creep? Manage lifecycle of system/process
	CFH Docmail Limited will only ever process the Trust's data as per explicit agreement with the Trust. The Trust and CFH Docmail Limited have a contract in place where roles and responsibilities are defined. There is limited scope to utilise the platform for other functions within the Trust. As data controller, the Trust has full responsibility for ensuring health care professionals accessing the system utilise it appropriately.

Stage - 3 Risk Template

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

Completed by	Gina Robinson	Role:	Information Security Officer	Date completed: 14th June 2022

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
Loss of system access due to connection failure or server failure either via NHIS or 3rd party supplier. This could result in the service being disrupted or unavailable. The consequences of this could be patient harm, financial penalties and reputational damage to the Trust	Full system back-up processes and ISO 27001 accreditation in place	2	2	4		2	2	4	Manual input, business continuity plan to be used
Loss of system data due to system failure and/or backup failure either via NHIS or 3rd party supplier. This could result in the service being disrupted or unavailable.	Full system back-up process in place. CFH Docmail Limited is ISO27001 and CE+ certified	3	1	3		3	1	3	Manual input, business continuity plan to be used

Risk description What event could happen which would impact on the activity? What would cause it to happen? What would the consequence be?	**Primary controls** What is in place now to prevent the risk from occurring or to act as a contingency if it does occur?	**Current risk**			**Gaps in control** If the risk is not controlled to an acceptable level, what are the issues that need to be addressed?	**Acceptable risk**			**Mitigating actions required** What needs to be done to reduce the risk to an acceptable level?
		Consequence	**Likelihood**	**Rating (C x L)**		**Consequence**	**Likelihood**	**Rating (C x L)**	
The consequences of this could be patient harm, financial penalties and reputational damage to the Trust									
Data is accessed inappropriately due to lack of access controls. Movers and leavers access not removed. Data is inappropriately processed and/or disclosed	Username and password controls in place. Account Management and access procedure completed. Appropriate access according to role. Segregation of duties. Research team will remove leavers from the system	2	2	4	Ensure access is managed and leavers list is received and actioned. Routine audits. Once a password is set it remains until the user changes it. CFH Docmail Limited will prompt for a password reset. The system requires a strong password	2	1	**2**	Ensure access is managed and leavers list is received and actioned. Routine audits. Users to regularly change their password in line with the Trust's Password Management Procedure
Business continuity plans in each area, do these exist and is there a template for recording if CFH Docmail Limited goes down.	Business Continuity plan for the CFH Docmail Limited system is in place	3	1	3		3	1	**3**	Business continuity plan reviewed annually.
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	In the Trust we have a business continuity plan if the service was unavailable. The department would default back to the current practice and manually address letters	2	2	4	CFH Docmail Limited will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO	2	1	**2**	CFH Docmail Limited will need to be added to the divisional information asset register and the data flows mapped and recorded as part of the annual IAO returns to the SIRO

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.