Information Sharing Gateway

iCode REALM

Data Protection Impact Assessment

DP010698

Created by Faith Okonkwo (NOTTINGHAM UNIVERSITY HOSPITALS NHS TRUST)

This PDF was generated on 10 May 2023 at 10:50 PM

Parties named in this Agreement

The Parties listed below recognise their responsibilities for ensuring this agreement complies with all legislation and other requirements relevant to the personal data being shared, including the specific governance measures set out in this DPIA.

Organisations Added

Organisation Name	Organisation Role	Assurance Status
NORTHAMPTON GENERAL HOSPITAL NHS TRUST	None Specified	Significant
KETTERING GENERAL HOSPITAL NHS FOUNDATION TRUST	None Specified	Significant
Chesterfield Royal Hospital NHS Foundation Trust	None Specified	Significant
University Hospitals of Leicester NHS Trust	None Specified	Expired
Sherwood Forest Hospitals NHS Foundation Trust	None Specified	Limited
University Hospitals of Derby & Burton NHS Foundation Trust	None Specified	Significant
NOTTINGHAM UNIVERSITY HOSPITALS NHS TRUST	None Specified	None
UNITED LINCOLNSHIRE HOSPITALS NHS TRUST	None Specified	Expired

Organisational Contributors Added

Organisation	Name	Roles
Chesterfield Royal Hospital NHS Foundation Trust	Eddie Lewis	Senior Officer, Administrator, Data Protection Officer
Chesterfield Royal Hospital NHS Foundation Trust	Dan Jones	
Chesterfield Royal Hospital NHS Foundation Trust	Terri Stubbins	Administrator, IG / Project Officer
KETTERING GENERAL HOSPITAL NHS FOUNDATION TRUST	Adam Brown	Administrator, IG / Project Officer, Data Protection Officer
NORTHAMPTON GENERAL HOSPITAL NHS TRUST	Sally Berrill	Administrator, Risk Reviewer, IG / Project Officer, Data Protection Officer
NORTHAMPTON GENERAL HOSPITAL	Sarah Stell	Administrator, IG / Project Officer, Data

NORTHAMPTON GENERAL HOSPITAL NHS TRUST	Sarah Steil	Administrator, IG / Project Officer, Data Protection Officer
NOTTINGHAM UNIVERSITY HOSPITALS NHS TRUST	Faith Okonkwo	IG / Project Officer
NOTTINGHAM UNIVERSITY HOSPITALS NHS TRUST	Roma Sejpal	IG / Project Officer
NOTTINGHAM UNIVERSITY HOSPITALS NHS TRUST	Jacqueline Moxon	IG / Project Officer
NOTTINGHAM UNIVERSITY HOSPITALS NHS TRUST	Barbara McCaffrey	Administrator, IG / Project Officer
NOTTINGHAM UNIVERSITY HOSPITALS NHS TRUST	Rory King	Senior Officer
NOTTINGHAM UNIVERSITY HOSPITALS NHS TRUST	Ian Saunderson-Darkes	Administrator
NOTTINGHAM UNIVERSITY HOSPITALS NHS TRUST	Andrea West	Administrator, IG / Project Officer
NOTTINGHAM UNIVERSITY HOSPITALS NHS TRUST	Precious Ojiako	IG / Project Officer
Sherwood Forest Hospitals NHS Foundation Trust	Jacquie Widdowson	Senior Officer, Administrator, Risk Reviewer, Data Protection Officer
UNITED LINCOLNSHIRE HOSPITALS NHS TRUST	DSP Team (NGH)	Administrator
UNITED LINCOLNSHIRE HOSPITALS NHS TRUST	Maria Dixon	Senior Officer, Administrator, Data Protection Officer
UNITED LINCOLNSHIRE HOSPITALS NHS TRUST	Ian Saunderson-Darkes	Senior Officer, Administrator
University Hospitals of Derby & Burton NHS Foundation Trust	Emily Griffiths	Administrator, Data Protection Officer
University Hospitals of Derby & Burton NHS Foundation Trust	Louise Shepherd	
University Hospitals of Leicester NHS Trust	Saiful Choudhury	Senior Officer, Administrator, Data Protection Officer

Purpose and Justification

Purpose

The Parties agree to use shared information only for the specific purposes set out in this document and to support the effective administration, audit, monitoring, regulatory inspection of services and reporting requirements.

The Parties accept that Shared information Shall not be regarded as general intelligence tor the further use by recipient organisations unless that further purpose is defined in this agreement and respective service users have been informed of this intended change of use.

The purpose, specific to this Data Protection Impact Assessment are identified as:

iCODE REALM solution facilitates and organises the execution of Radiology Events And Learning Meetings (REALM) leading to improved professional practice and raising the standards of patient care and safety through a learning process.

Benefits

The benefits, specific to this Data Protection Impact Assessment are identified as:

iCODE REALM has been developed according to the Royal College of Radiologists (RCR) guidelines and recommended standards. It is a vendor neutral solution integrated into a PACS environment to manage and organize REALMs. Benefits are: Streamlined REALM meeting workflow Data Anonymization Time and resource efficiency Reduce workload challenges Easy to access and simple to use Powerful meeting management tools Analytics and Reporting

It is recognised that unless the law specifically requires or permits, this shared information will not be used for different purposes or further disclosed. Even where the law permits further disclosure, in line with good practice the originating data controller Will be consulted first and depending on the circumstances, it may be necessary for the data subject to be informed of the disclosure.

Screening Outcome

The information below shows the answers given within this DPIA screening questions.

Question	Answer
Will the activity involve the use of personal data and includes pseudonymised data?	Yes
Will the activity be using special categories or criminal offence data?	No
Will the activity include the use of personal data of vulnerable persons, such as children or vulnerable adults?	No
Will the activity use new or existing personal data for a purpose an individual is not aware of or	No

in a way it is not currently used changing its nature, scope, context or purpose?	
Will the activity involve the use of innovative technologies or the application of existing technologies, that could be perceived as privacy intrusive or novel?	No
Will the activity involve the monitoring of publicly accessible places for example use of CCTV?	No
Will activity use biometric or genetic data?	No
Will the activity track individuals location or behaviours such as physical location or online presence?	No
Will the activity involve data matching, combining, comparing or matching personal data from different or multiple sources?	No
Will the activity introduce a risk that the use of personal data may cause harm, distress, damage or loss of control of their data for the individual?	No
Will the activity include the evaluating, scoring or profiling of an individual?	No
Will the activity use automated processing and includes profiling in order to make decisions about individuals?	No
Could the activity prevent an individual exercising their legal rights or lead to a denial of a product, service, opportunity or a benefit?	No

Information within the DPIA template

Detail the Processing Activity

Scope and Purpose

Summarise the type of activity that will be taking place and why it needs to be implemented or changed

All doctors in clinical practice within EMRAD Trusts have a duty to participate in personal learning and development. Radiology Events And Learning Meetings (REALM) are a form of clinical review held within each Trust not cross-Trust to enhance patient safety and learn from clinical outcomes. Only the chair of a REALM, who always has a legitimate clinical relationship with the patients being discussed, will be able to identify any patients. Other members of the REALM will only see anonymised patient information, and no information from the REALM should be shared with any other process. Extremely rarely, it may be necessary for the REALM chair to involve wider clinical teams for a particular patient if it felt by the meeting that there is an urgent and previously unrecognised finding that will impact on patient safety imminently. REALM is currently done manually. iCODE REALM will follow a phased implementation plan per trust to streamline and automate the process followed by EMRAD trusts and alleviate some manual resources required to schedule, run and document REALM meetings. UPGRADE Pending 1) This upgrade allows the REALM Chair to add cases, reviewed prior to Go Live with REALM. These cases will have to be added manually. Prior to this recent upgrade, this would not have been possible. 2) This upgrade will also help to maintain the special characters within the body of the report once encrypted by Rosenfield. This feature will help remove the risk of report being altered. 3) Following the upgrade, modalities can be viewed in specific folders allowing audit and learning for each modality. This will allow the REALM Chair to have an overall view across all modalities. This new feature will also allow additional sub REALM meetings to take place with designated individuals. 4) Upgrade gives the possibility of adding a timeout warning pop-up safety feature 5) An extra feature has now been added allowing an individual the facility to search for meetings assigned to a specific sub-folder in the Calendar page 6) An extra feature has now been added allowing an individual to search for meetings using a meeting's sub-folder and/or cases' sub-folder in the History module 7) This Upgrade has no impact on costs, data storage & also there will be no system downtime during the process of upgrade. It will be installed on the test environment first and once this is validated by the trusts an RFC for all EMRAD trusts will be raised by GE to add this into the LiveEnv

Which statements best reflects this purpose?

- Introducing a new system or technology

iCODE REALM solution facilitates and organises the execution of Radiology Events And Learning Meetings (REALM) leading to improved professional practice and raising the standards of patient care and safety through a learning process.

What are the benefits that will be realised from the intended outcome?

iCODE REALM has been developed according to the Royal College of Radiologists (RCR) guidelines and recommended standards. It is a vendor neutral solution integrated into a PACS environment to manage and organize REALMs. Benefits are: Streamlined REALM meeting workflow Data Anonymization Time and resource efficiency Reduce workload challenges Easy to access and simple to use Powerful meeting management tools Analytics and Reporting

Who benefits and why?

Patients direct care will be improved and also EMRAD's Radiology Department will benefit by having a consistent process across the patch thereby resulting in time and resource efficiency.

What are the risks should the data collection and use not take place?

REAL Cases will be uploaded manually and this will increase the risk of data availability without anonymization. This is a recommended process which will standardise the recording of cases and clinical learning across EMRAD trusts. By not using this software patient care, improvement and learning may be compromised

What information assets are involved in the activity?

PACS

Which personal data items are being collected (including pseudonymised)?

None Specified

Which special category data items are being collected?

- Physical / Mental Health or Condition

Will you be collecting or using data for a law enforcement purpose?

No

Will it involve automated processing or profiling?

No

Will it be used solely within your organisation or shared outside your organisation?

- Internal

What is the frequency of the transfer?

Monthly

How many records are being transferred?

Transfer - 11-50

Who does the data relate to?

- Patients
- Staff (NOT including volunteers, agents, temporary and casual workers)

Patient images only. There is no demographics included. Staff user names will also be included as part of the data contained in iCODE REALM.

What is the direction of the data flow?

Bi-directional to/from. Internal - On site

How many records does the collection or use relate to?

11-50

How many data subjects does the collection or use relate to?

11-50

What is the format of the data when collected or used?

- Electronic System - Structured e.g. coded data

How often will the data be collected or used?

Monthly

How long will the data be collected or used for? Please select a date or enter a time period

29 September 2024

Data usage is ongoing for the initial contractual period and will be extended based on the contract agreement. However, during this period the REALM chair will do a regular review of cases and would delete cases that are no longer needed. Data is all anonymised.

What geographical area does the collection or use cover?

East Midlands Region in the UK - EMRAD Trusts

How will you prevent function creep?

Functionalities are restricted with the solution and external users are not given access, only NHS users with AD Login will have access to the system. Amend to Functionalities are restricted with the solution and external users are not given access, only NHS users with AD Login by default but they must have active accounts on iCode REALM as well will have access to the system.

Have you considered any alternatives to this activity and assessed why this method is the most appropriate?

Yes

The alternative is a paper based local option which is un-auditable and labour intensive for managing.

Nature

How will the data be collected?

- Digital information system

Images from PACS will be anonymised and transferred to iCODE REALM. Anonymisation takes place automatically during the transfer of images from PACS to ICODE REALM. Technical workflow from Rosenfield attached for reference.

Where will the data be stored and used after collection?

- Secure storage on organisations premises
- Server - system on organisation premises

iCODE REALM server will be installed on the hospital's or Imaging Network's data center which will provide REALM functionalities for single hospital or multiple hospitals under an imaging network.

How long will it be stored as a minimum? Please select a date or enter a time period

28 September 2024

24.00

Who will have access to the data?

- Other

Radiology Department

Are there measures in place to support third parties?

No

Context

Are these data subjects classed as vulnerable e.g. a child or vulnerable adult?

No

Who is the source of the data collected and used?

- Other

Images are originally collected from Patients and stored on PACS, a selected image is therefore transferred from PACS to ICODE REALM when required

What are the relationships between the individuals?

NHS Patients

Is the collection and use of the data expected by the individuals?

Yes

Fair Processing Notice (or Privacy Notice) on the Trusts public website covers this. All doctors in clinical practice within EMRAD Trusts have a duty to participate in personal learning and development. Radiology events and learning meetings (REALM) are a form of clinical review held within each Trust to enhance patient safety and learn from clinical outcomes. Only the chair of a REALM, who always has a legitimate clinical relationship with the patients being discussed, will be able to identify any patients. Other members of the REALM will only see anonymised patient information, and no information from the REALM should be shared with any other process. Extremely rarely, it may be necessary for the REALM chair to involve wider clinical teams for a particular patient if it felt by the meeting that there is an urgent and previously unrecognised finding that will impact on patient safety imminently.

Please describe any previous experience involved parties may have in using or collecting data.

REALM is currently done manually. iCODE REALM is being implemented to streamline and automate part of the process followed by EMRAD trusts

Could this activity be seen as high risk to the data subjects?

No

Is there complaince with any UK GDPR Codes of Conduct or certifcation schemes?

N/A

Necessity and Proportionality

Lawfulness

What is the lawful basis for the personal data for collection and use?

- Task carried out in the public interest / authority vested in the controller

What is the lawful basis for the special category data for collection and use?

- Necessary for medical purposes

What is the lawful basis for the law enforcement data for collection and use?

- Necessary for archiving, research or statistical purposes - Schedule 8 (9)

What is the Legal Gateway for the collection and use?

NHS ACT 2006

Individual Rights

Right to be informed – Please describe the process?

Each EMRAD Trust has a privacy notice to inform data subjects about what they do with their personal data.

Right of Access – Please describe the process?

Each EMRAD Trust has approved processes in place for providing data subject access to their personal data, within the required timescale.

Right to rectification – Please describe the process?

Each EMRAD Trust has approved processes in place for considering data subject requests to rectify data held about them.

Right to erasure – Please describe the process?

Right to restriction processing - Please describe the process?

Each EMRAD Trust has approved processes in place for considering data subject requests to restrict the processing of their data.

Right to object – Please describe the process?

Each EMRAD Trust has approved processes in place for considering data subject objections to how their data is processed.

Rights relating to automated decision making including Profiling - Please describe the process?

Not Applicable

Data Standards

Describe how the data is adequate, relevant and limited to what is necessary to fulfil the purpose of the data collection

As data is being used for learning, only the relevant images which are seen as a near miss or golden spot are uploaded onto the iCODE REALM and images are anonymised automatically during the upload process.

Select one or more statement to describe how the data will be kept up to date and checked for accuracy and completeness

- Other

Anonymised images are stored with no patient identifying data attached. Images can be removed when required do so

Describe how this retention schedule is supported

- Other

No personal data will be stored on application only anonymised Images will be deleted according to NHS Trust policy

Select one or more to describe how data is shared or disclosed?

- On site viewing

Only users with access to the application can have the access to view data

Security

Will the data be transferred outside of the UK?

No

Select one or more statements to describe what controls are in place to manage the security risk?

- All polices and measures are regularly reviewed and update appropriately
- Any data processor used also implement appropriate technical and organisational measures
- Implemented Information security policy (or equivalent) and where necessary additional policies to enforce controls
- Record of processing activity and the assets used
- Risk management process in place to analyses and assess the appropriate level of security
- Take account of the state of the art and costs of implementation when deciding on measures

Data Policies are in place within EMRAD and also individual trust have their data policies in place to manage security risks. Also as this sits in PACS it's also within PACS security.

Select one or more statement to describe what controls are in place to protect against cyber-attacks?

- Access to the data is controlled and limited to those who have a legitimate need to access with adequate audit trails and unused accounts are either disabled, suspended or removed
- Actively monitor software vulnerabilities, such as in-support software, security patch updates, and mitigation where patches cannot be applied
- Basic technical controls such as those specified by established frameworks like Cyber Essentials or equivalent
- Control how devices are connected such as network access controls
- Encrypting data at rest on mobile devices that are not subject to strong physical controls
- Encrypting data in transit
- Ensure the environment is secure throughout its lifecycle
- Manage end user devices such as laptop and smartphones to use approved and assured software
- Privileged accounts are limited with two factor authentication considered
- Robust password policy that uses National Cyber Security Centre best practice to avoid weak guessable passwords and all default passwords are changed
- Staff trained in data security on at least an annual basis with refresher training as required
- Track and record all assets that use personal data including end-user and removable media
- Undertake regular testing to evaluate the security measures, including virus and malware scanning, vulnerability scanning and conduct penetration tests
- Use technical controls such as encryption to prevent unauthorised or unlawful access
- Use where necessary technology to prevent downloading, transferring. Altering or deleting data
- Web services are protected from common security vulnerabilities using publications such as OWASP
- Other

Dual layer firewalls with restricted access to only the required servers and ports is in place only allowing access to the applications from the approved trust ranges. Security zone segregation within the firewalls is in place to separate application and protected data so only required access is allowed between server components. Included in the core firewall infrastructure is the intrusion detection system (IDS), this monitors all traffic incoming to the DC is monitored for unusual traffic patterns and alerts are sent for anomalous traffic. In addition all servers are protected by MacAfee Crowd Strike Falcon, this software monitors for malicious software and viruses on the server infrastructure.

Select one or more statements to describe what controls are in place to detect security events?

- Monitor the status of the system
- Monitor user activity with transactions being attributed to an individual user
- Other

The Central Datacentre IDS System is configured to alert upon detection of unusual traffic patterns. The DC operations team monitor and report on these activities on daily basis to the DC Operations manager. The alert is also sent to the GE Security team of the activity as it occurs. Crowd Strike Falcon also alerts the GE Corporate Security team of alerts and this triggers an internal security event.

Select one or more statements to describe what controls are in place to minimise the impact?

- Incident management processes in place which includes root cause analysis, lesson learned and approach to reporting to appropriate bodies (ICO)
- Regular testing and review measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement
- Restore access to personal data in the event of any incidents, e.g. backup process and disaster recovery
- Other

The security response team monitor the alerts and instigate a security event. The IDS System can block the malicious traffic upon validation by the GE engineers. The Crowd Strike Falcon software can quarantine the workstation of suspicious software automatically upon detection. In critical enterprise wide issues the IDS and firewalls can restrict access to/from locations to stop propagation.

For CCTV select one or more statements that is documented in a policy which supports the use of CCTV

- Other

Not Applicable

Risk Assessment

Question	Description	Controls	Initial Rating	Action	Final Rating
	The assurance of one or more of your partner organisations named has either expired, is limited or hasn't been submitted within the system. It is recommended that data sharing partners provide significant assurance on their practices or provide evidence to support assurance. You should ensure that the necessary due diligence and checks are made.	Missing controls: • All organisations in DPIA should have significant assurance or provide evidence to support assurance.	High	Mitigate / reduce Assurance is mostly provided via the Data Security and Protection Toolkit (DSPT). Trust partners (SFH, NUH and UHL) are working towards DSPT compliance through action improvement plans as these 3 Trusts have a status of 'Approaching Standards', which means that they have not met all requirements. All 3 trusts have an improvement plan agreed by NHSD.	Low
1.2.3	Servers hosted within the UK are bound by UK Law and legislation. You must ensure that the necessary due diligence and checks are made. Make sure access is controlled.	Controls in place: • Server - system on organisation premises • Secure storage on organisations premises	Low	Accept / tolerate Servers are held in GE UK Datacentre	Low
1.2.7	There are no measure and controls in place to support processing		High	Mitigate / reduce The supplier Rosenfield is a	Low

	by Third Parties, which are required to ensure that the data is processed under the Controller instruction and appropriate technical and organisational controls are in place.			third party contract, managed via back to back data processing agreement with GE who is our prime data processor. All data processed as part of this implementation is stored in the EMRAD VNA in the GE Datacentre in the UK. Access to the product is managed via Active Directory and assigned access roles.	
1.3.1	Data subjects are not classed as vulnerable e.g. a child or vulnerable adult.		Low	Accept / tolerate All data subjects are managed with the same process of de-identification before uploading data. There would be options as per local trust processes for data opt out if required.	Low
1.3.4	The collection and use of the data is expected by the individuals.		Low	Accept / tolerate Data used during the REALM process is anonymised.	Low
1.3.6	This activity is not seen as high risk to the data subjects.		Low	Accept / tolerate As this product	Low

				is designed to support patient care through the process of Education and Learning, this is not expected to be identified as a high risk from the data subjects. A replica manual process has been used for many years.	
1.1.23	Alternatives have been reviewed and this has been assessed to be the most appropriate.		Low	Accept / tolerate The alternative is a paper based local option which is un-auditable and labour intensive for managing.	Low
2.8.2	Data should be up to date and checked for accuracy and completeness. Not all recommended controls have been selected.	Controls in place: • Process which supports regular checks for accuracy of the data collected and when this should take place, including the source of the data Missing controls: • Where errors are detected or mistakes made, there is the ability to record as such • Where data is clearly an opinion, whose opinion is noted and any changes to the underlying fact • Where appropriate, comply with a subject right to rectification and carefully consider any challenges to the	Significant	Change Data uploaded for REALM is provided from downstream systems that already have local processes to ensure accurate data quality. If Patient details are identified as incorrect, they should be changed in the primary system by the local organisation. The Imaging Network uses a product called ICW to manage mis-matches in the MPI (Master Patient	Low

		accuracy of the data, which is noted.		Index).	
2.8.3	CCTV images should have appropriate controls to ensure the images are not retained for longer than necessary and are disposed of securely. Not all recommended controls have been selected.	Controls in place: • Data reviewed at minimum retention and decision made as to next step Missing controls: • Data automatically deleted after retentions period • Deletion required initiation • Under certain circumstances, authorised persons may override	Significant	Change Not Applicable	Low
2.9.3	The recommended controls support the management of security risks.	Controls in place: • Implemented Information security policy (or equivalent) and where necessary additional policies to enforce controls • All polices and measures are regularly reviewed and update appropriately • Record of processing activity and the assets used • Risk management process in place to analyses and assess the appropriate level of security • Take account of the state of the art and costs of implementation when deciding on measures • Any data processor used also implement appropriate technical and organisational measures	Low	Accept / tolerate	Low

2.9.4	The recommended controls support protection against cyber-attacks.	Controls in place: • Basic technical controls such as those specified by established frameworks like Cyber Essentials or equivalent • Access to the data is controlled and limited to those who have a legitimate need to access with adequate audit trails and unused accounts are either disabled, suspended or removed • Privileged accounts are limited with two factor authentication considered • Use where necessary technology to prevent downloading, transferring. Altering or deleting data • Robust password policy that uses National Cyber Security Centre best practice to avoid weak guessable passwords and all default passwords are changed • Use technical controls such as encryption to prevent unauthorised or unlawful access • Track and record all assets that use personal data including end-user and removable media • Control how devices are connected such	Low	Accept / tolerate Access to data through legitimate access. Data stored in GE London datacentre monitored by Onwatch (GE proprietary system to monitor uptake an access)	Low

		as network access controls • Actively monitor software vulnerabilities, such as in-support software, security patch updates, and mitigation where patches cannot be applied • Manage end user devices such as laptop and smartphones to use approved and assured software • Encrypting data at rest on mobile devices that are not subject to strong physical controls • Encrypting data in transit • Web services are protected from common security vulnerabilities using publications such as OWASP • Ensure the environment is secure throughout its lifecycle • Undertake regular testing to evaluate the security measures, including virus and malware scanning, vulnerability scanning and conduct penetration tests • Staff trained in data security on at least an annual basis with refresher training as required • Other - Dual layer firewalls with restricted access to only the required servers and ports is			

		in place only allowing access to the applications from the approved trust ranges. Security zone segregation within the firewalls is in place to separate application and protected data so only required access is all			
2.9.5	The recommended controls support the detection of security incidents.	Controls in place: • Monitor user activity with transactions being attributed to an individual user • Monitor the status of the system • Other - The Central Datacentre IDS System is configured to alert upon detection of unusual traffic patterns. The DC operations team monitor and report on these activities on daily basis to the DC Operations manager. The alert is also sent to the GE Security team of the activity as it occurs. Crowd Strike Falcon also alerts the GE Corporate Security team of alerts and this triggers an internal security event.	Low	Accept / tolerate Access is controlled via active directory. Audit facility is available through role based access.	Low
2.9.6	The recommended controls help minimise the impact of security incidents.	Controls in place: • Incident management processes in place which includes root cause analysis, lesson learned and approach to reporting to appropriate bodies	Low	Accept / tolerate Incident Management Processes via EMRAD Business As Usual team and GE adhering to	Low

		appropriate bodies (ICO) • Restore access to personal data in the event of any incidents, e.g. backup process and disaster recovery • Regular testing and review measures to ensure they remain effective, and act on the results of those tests where they highlight areas for improvement • Other - The security response team monitor the alerts and instigate a security event. The IDS System can block the malicious traffic upon validation by the GE engineers. The Crowd Strike Falcon software can quarantine the workstation of suspicious software automatically upon detection. In critical enterprise wide issues the IDS and firewalls can restrict access to/from locations to stop propagation.		ITIL	
	Lack of engagement from some trusts	Currently working with 4 trusts (KGH, UHDB, SFH and CRH) who are fully engaged and the plan is to fully implement iCODE REALM in these 4 trusts and then work with remaining trusts (NGH, NUH, ULH, UHL) following the initial implementation. Wc 21/11/2022 - We now have engagement from NGH and UHL as well. Gradually progressing with	Significant	Mitigate / reduce	Low

		both these trusts.			

Outstanding Tasks

Task ID	Assigned To	Created By	Created On
TA000798	Saiful Choudhury	Roma Sejpal	07 Oct 2022
TA000799	DSP Team (NGH)	Roma Sejpal	07 Oct 2022
TA001287	Sarah Stell	Roma Sejpal	10 May 2023
TA001288	Eddie Lewis	Roma Sejpal	10 May 2023
TA001289	Emily Griffiths	Roma Sejpal	10 May 2023
TA001290	Jacquie Widdowson	Roma Sejpal	10 May 2023
TA001291	Saiful Choudhury	Roma Sejpal	10 May 2023
TA001292	Ian Saunderson-Darkes	Roma Sejpal	10 May 2023

Additional Documents

Linked Question	File Name	Added By	Added On
	HCD-ISO-27001-certificate-2025_IS-505218-1.pdf	Roma Sejpal	06/09/2022 08:00:22
	iCode REALM - Admin Manual - Version 2.2 .pdf	Roma Sejpal	23/11/2022 14:57:41
	iCODE REALM - GO LIVE Dependencies and Actions.msg	Roma Sejpal	21/11/2022 10:19:14
	iCode REALM - Local REALM Chair Manual - Version 2.2 .pdf	Roma Sejpal	23/11/2022 14:57:41
	iCode REALM - Local User Manual - Version 2.2.pdf	Roma Sejpal	23/11/2022 14:57:41
	iCode REALM User Types Defined.pdf	Roma	18/11/2022

		Sejpal	10:00:03
	ROSENFIELD DWC LLC ISO 9001-2015.pdf	Roma Sejpal	06/09/2022 08:00:52
1.1.7	iCODE REALM - Data Gathering Query.msg	Roma Sejpal	26/10/2022 09:40:31
1.2.1	iCODE REALM - Data Gathering Query.msg	Roma Sejpal	26/10/2022 10:16:57
1.2.1	iCode REALM Technical Details.pdf	Roma Sejpal	20/11/2022 21:42:30

Executive Summary

Below is what is detailed within the Executive Summary in the Approvals tab of the DPIA:

Approvals

Contributor	Organisation	Requested	Review By	Reviewed On	Outcome
There are no approvals for this DPIA					

DPIA Finalisation

The date this DPIA was finalised on is:

The following ISAs have been created from this DPIA:

None