Royal Devon
University Healthcare
NHS Foundation Trust

Datix DPIA

Reference Number: RDF1202-23
Date of Response: 30/01/2023

Further to your Freedom of Information Act request, please find the Trust's response(s) below:

Please provide a copy of any Data Protection Impact Assessment conducted by you, or (if relevant) any pre-decessor authority into the use of RL Datix, Datix Cloud, or migration from onsite Datix to Datix Cloud.

Please find attached.

Please note the following Exemptions have been applied to this Trust response:-

Section 31(3) of the FOIA.
The Trust has removed the check list, risk assessment and information asset register tab. The Trust cannot provide this requested information under Section 31(3) of the FOIA. Section 31(3) of the Freedom of Information Act allows a public authority to neither confirm nor deny whether it holds information where such confirmation would be likely to prejudice any of the matters outlined in section 31(1). This includes information the disclosure of which would or would be likely to prejudice the prevention or detection of crime. Section 31(3) is subject to a public interest test for determining whether the public interest lies in confirming if the information is held or not.

Factors in favour of confirming or denying the information is held.

The Trust considers that to release the requested information would reveal details that could assist in a cyber-attack. However the Trust recognises that answering the request would promote openness and transparency with regards to the Trust's IT security.

Cyber-attacks which may amount to criminal offences under the Computer Misuse Act 1990 or the Data Protection Act 2018, are rated as a Tier 1 threat by the UK Government. The Trust like any organisation may be subject to cyber-attacks and since it holds large amounts of sensitive, personal, and confidential information, maintaining the security of this information is extremely important.

In this context, the Trust considers that providing the requested information would also provide information about the Trust's information systems and its resilience to cyber-attacks. There is a very strong public interest in preventing the Trust's information systems from being subject to cyber-attacks. Releasing the type of information requested would be likely to prejudice the prevention of cybercrime, and this is not in the public interest.

As an Operator of Essential Services: (https://www.legislation.gov.uk/uksi/2018/506/schedule/2/paragraph/8), the Trust must comply with The Network and Information Systems Regulations 2018. By releasing information that could increase the likelihood or severity of a cyber-attack, the Trust would fail to meet its security duties as stated in section 10 (https://www.legislation.gov.uk/uksi/2018/506/regulation/10) of the Network and Information Systems Regulations 2018.

The prejudice in complying with Section 31(3) of FOIA is real and significant and would allow valuable insight into the perceived strengths and weaknesses of the Trust's IT infrastructure and information systems.

Section 40 (2) – Personal Data and Section 40 (3a)

We have also redacted/edited out any contact information contained in the document.

The Trust believes that the release of such sensitive information meets the definition of personal data and disclosing the information would contravene one of the data protection principles set out in Article 5 of the UK GDPR. As such release of the information would be likely to cause distress to the individuals concerned.

The disclosure of staff names would breach the first data protection principle and fail to meet any of the relevant conditions set out in Schedule 2 of the Data Protection Act (DPA) 2018. The first principle in the DPA requires that disclosure must be fair and lawful, and, in particular, personal data shall not be processed unless at least one of the conditions in Schedule 2 is satisfied. The staff concerned would not have expected their names to be disclosed in the public domain and so disclosure would not be 'fair' in the manner contemplated by the DPA. Furthermore, disclosure would not satisfy any of the conditions for data processing set out in Schedule 2 of the DPA. In particular, we do not consider that there is a legitimate interest in disclosure in this case. There is no public interest in making information about our staff available in this way contrary to what would have been their legitimate expectation at the time the information was gathered.

Royal Devon & Exeter NHS Foundation Trust
Data Protection Impact Assessment Toolkit

Version: 4 **Updated Apr 2021**

Data Protection Impact Assessment (DPIA) is a tool used by organisations at the design stages of a project, in order to ensure that data protection and privacy risks are identified and mitigated prior to implementation. An effective DPIA ensures that projects which process personal data meet an organisation's statutory requirements under both the Data Protection Act 2018 (DPA), General Data Protection Regulation (GDPR) 2016 and the Human Rights Act 1998 (HRA).

A DPIA should be considered wherever a new system or service is planned, or a when a change is proposed to how an existing one works; for example, when:

- Building a new IT system for storing or accessing personal data
- Developing policies or strategies that have privacy implications
- Embarking on a data sharing initiative
- Using data for new purposes

Please complete all questions with as much detail as possible. For most DPIAs it would be useful for a process document or user guide to be attached so that anyone considering the DPIA can see how it will be used on a day to day basis. Start to fill out the template at the beginning of any major project involving the use
of personal data, or if you are making a significant change to an existing process. Integrate the final outcomes back into your project plan.

Guidance:
See the Check sheet for guidance on requirments and links for more information
More info on the Hub page:
If you need further information please contact the Information Governance Office

Name of Contact (eg DPO, IT Security etc)	Date Reviewed	Outcome	Comment
DPO -			
Head of IG - Northern -			
Head of IG - Eastern -			
IG Lead - Northern -			
IG Lead - Eastern -	**12/04/2022**	**Recommend approval**	**DPIA completed for system level and supporting documents supplied in zip folder - note cyber essentials certificate has expired - asked project lead if there is a more up to date one. Updated certificate supplied**
Cyber Security Manager -	19/04/2022	Approved	
Caldicott Guardian -	19/04/2022	Approved	
ISF Members - redacted			
Other - such as project board if relevant			

Name of Forum	Date Reviewed	Outcome	Comment
Information Security Forum	19/04/2022	Approved	
Information Governance Steering Group	23/05/2022	Approved	Ratified

DPIA Completed by	
Job Title	Safety and Risk Systems Manager
Email Address and contact number	
Information Asset Owner (IAO)	
Senior Staff Members/Committees endorsing this project	

COVID Questions	
Is this being set up as part of COVID-19 response? Please complete as much as possible including the risk assessment and contact the IG team for advice, urgent approval can be obtained by IT Security, DPO and Caldicott Guardian outside of normal process if required.	No
Is this required to continue once COVID-19 response is complete? A review of the asset will be required once no longer required for COVID to understand decommissioning or moving into standard service.	No

Please note the section below will be published on the Trust website

Royal Devon & Exeter NHS Foundation Trust
Data Protection Impact Assessment Toolkit Version 4

DPIA Reference	*DPIA1230*
DPIA Title	Datix Cloud IQ - System Information
Summary of Proposal This is provided to Information Governance Steering Group and Satefy and Risk as an overview of the project. It is also published on the website and should provide the public with an understanding of the information asset and how data is protected as a standalone statement.	The proposal is to move RDE and NDHT onto 1 joint Datix Licence and to use one Datix Cloud IQ organisation across both organisations The RD&E had planned to move the capture (incidents, complaints and claims) modules from Datix Web to DCIQ by December 2021, as early stage construction/development had commenced. However, following the report to the joint Governance Committee this work was paused and the Safety and Risk System Manager at the RD&E was commissioned by the RD&E Interim Chief Nurse to outline the benefits of a collaborative approach to move both trusts from web to DCIQ simultaneously. The decision has been made to move to DCIQ as part of the intergration programme. This will cover RD&E and NDHT for the following 5 modules: 1. Incidents 2. Feedback (complaints, PALS and compliments) 3. Claims 4. Enterprise Risk Manager (risk registers) 5. Mortality DCIQ is beneficial as it will offer a wider range of capability in terms of reporting functions, more connectivity (one module will link to another for example mortality records will be able to link to risk and/or incidents). It will also offer the opportunity to purchase additional modules to support investigation, trending and theming activity DPIA to be continue to be reviewed with changes with the national reporting system for incidents changing from NRLS to LFPSE. This may mean incidents direct upload from DCIQ to the new national reporting system, DPIA to be reviewed and bought back when this work is out of trial stage nationally. Further updates https://www.england.nhs.uk/patient-safety/learn-from-patient-safety-events-service/
Date Ratified	
Date Ratified	23 May 2022

1	Summary of Processing Activity	Response	ISF Feedback
1.1	Will identifiable personal data be processed as part of this project?	Yes - details of the personal data will be captured at module level. This DPIA is system level and access only 1. Incidents - Datix DPIA 2. Feedback/Complaints - Datix DPIA 3. Claims - Datix DPIA 4. Mortality - Datix DPIA 5. Risk - Datix DPIA This section to be updated if further modules are purchased within the DCIQ system	
1.2	Please list the data elements that will be used as part of this project (e.g.; name, address, national insurance number, medical diagnosis and treatment details, etc.)	User details for access: Name Job title Email address AD account Location and use groups linked to Work phone number system use audits	
1.3	Will any of the following "special categories" of personal data be processed as part of this project (please list all categories): • racial or ethnic origin • political opinions • religious or philosophical beliefs • trade union membership • health • sex life or sexual orientation • genetic or biometric data for the purpose of uniquely identifying an individual	n/a - This DPIA to review system only please see linked DPIAs for this information	
1.4	Please categorise who the information is about (e.g.; dialysis patients, medical staff, etc.)	Staff at RDE and NDHT, Sodexo staff (NDHT only), Castleplace, Chime	
1.5	Please justify why it is necessary for this personal data to be processed	user to access the system and granular access to relevant areas. Email address to notify staff member of relevant incident/feedback.	
1.6	Please describe how this information will be obtained and who from	all access to modules is granted by access to profiles linked to their location of work or specialist role (e.g. Tissue viability, Radiation etc) RDE - linked to AD NDHT - manual until ADs integrated or DCIQ capable of linking to multiple ADs Governance manager or staff manager can request access via contacting risk management	
1.7	Please describe how/where this information will be stored	Hosted by AWS, stored in London. Centrify (system that links DCIQ to RDE AD) which runs log in details/information, cache data of username and email address in Amsterdam. Connectivity currently through N3, IT working with Datix to narrow down access to the system to site wide IP addresses	
1.8	Please describe which RD&E staff will process this information as part of the project and what processing activities they will undertake (e.g.; viewing, amending, sharing etc.)	Users managed by Safety Systems team (Mark, Bec, Kerry)	
1.9	Please describe all third party organisations that this information will be shared with, what data will be shared and why. It is also useful to include details of any contracts or data sharing agreements in place to support this.	RLDatix - system supplier Contract available on request	
1.10	Does this project require the installation of new software?	No - this is cloud based and already in use for Mortality DPIA - 1138 approved 20th August 2020	*Add ref number*
1.11	Does the project / process involve new linkage of personal data with data in other collections, or significant changes in data linkages? If 'yes', please provide details.	Only links to AD for access.	

2	Fairness, Transparency and Lawful Bases	Response	ISF Feedback
2.1	Is this already covered by the RDE Privacy notices and should it be amended? If not how will data subjects be told about how their personal data will be used as part of this project? *RDE privacy notices are published at: https://www.rdehospital.nhs.uk/about-us/information-governance/fair-collection-privacy-notice/*	Yes, no new data, all already covered in current Datix	

2.2	Article 6 Condition of Processing: What lawful basis is the Trust relying upon to process this personal data for this project? *If the processing of the information in this information asset is necessary for undertaking statutory functions, such as primary healthcare, answer "6(1)(e) Official Authority".*	6(1)(e) – Official authority	
2.3	Article 9 Condition for Processing: If processing special categories of personal data for this project, what further lawful basis is the Trust relying upon? *If the processing of the information in this information asset is necessary for delivering healthcare/treatment, answer "9(2)(h) Health and Social Care..."*		*See each module for condition for special category. N/A to system level.*

3	Compatible Purposes	Response	ISF Feedback
3.1	Is the proposed processing of this personal data different to what data subjects will have been told when their information was collected?	No	
3.2	If so, how will data subjects be told about the changes?	N/A	

4	Adequacy & Relevance	Response	ISF Feedback
4.1	Is the personal data of good enough quality to serve the purpose?	Yes	
4.2	Has the use of anonymous data been explored? If so explain why this is not viable.	no - need user details to manage access	
4.3	Please explain what measures are in place to ensure that the amount of personal data processed will not exceed the minimum essential for the purpose	limited to user data to manage access	

5	Accuracy of Data	Response	ISF Feedback
5.1	Is it possible to amend or update the personal data being used as part of this project?	Yes - list of changes for starters, leavers, movers	
5.2	Please outline the steps that will be taken to ensure the accuracy of any personal data that is used as part of this project	users notify where there are access issues	

6	Retention	Response	ISF Feedback
6.1	Have retention periods been set for personal data used as part of this project?	No	
6.2	What are the retention periods for the data? Where this is included in the Records Management Code of Practice please list all records type *https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/*	Audit logs retained for 3 years. Leavers hidden and then removed periodically (every 3 years) to cleanse the system	
6.3	How will the data be destroyed at the end of its retention period?	Delete and remove backup	

7	Data Subject's Rights	Response	ISF Feedback
7.1	Who will facilitate requests for access to the personal data being processed as part of this project? *(Requests are usually processed by the Trust IG team - please record how the IG team can access the information or provide a point of contact for requests to be actioned)*	Safety and Risk Team	
7.2	What measures have been put in place to ensure that information can be easily extracted and provided in response to a subject access request?	Reports and investigation templates set up. All data exportable into excel or word templates.	
7.3	Do you intend to send direct marketing messages by electronic means? This includes both live and pre-recorded telephone calls, fax, email, text message and picture (including video)?	No	
7.4	Are there procedures in place for an individual’s request to prevent processing for purposes of direct marketing in place?	n/a	
7.5	Will automated decisions be taken about data subjects, without manual checking and if so, is this outlined in the privacy notice?	No	
7.6	Will the processing be likely to cause individuals damage or distress? In what way? *(is this is their reasonable expectations if not consider distress)*	No	
7.7	What procedures are in place for the rectifying / blocking / erasure / destruction of data by individual request or court order?	Users not given permission to delete data	

8	Security	Response	ISF Feedback

8.1	Is a third party organisation being used to process personal data on behalf of the Trust (a data processor), as part of this project? *(Please provide copies of contractual/assurance documents or reference number in procurement database)*	Yes	
8.2	If 'yes', does the contract with the data processor contain all of the necessary Trust Information Governance clauses? *(NHS Standard Contract should be used, Procurement can help with this)*	Yes	
8.3	Has the data processor registered as a data controller with the Information Commissioner's Office? If 'yes', what is their registration number? *See: https://ico.org.uk/ESDWebPages/search/*	Yes Z8100369	
8.4	Has the data processor completed a Data Security & Protection Toolkit submission? If so what is their ODS and latest status? See: https://www.dsptoolkit.nhs.uk/OrganisationSearch	Yes 8HD22	
8.5	Is there a useable audit trail in place for the system and what information does this provide (e.g.; record of who has accessed a record)	Yes full audit trail	
8.6	By what method(s) will information be transferred?	AES-256 encryption	
8.7	What measures are in place to ensure the security of information being transferred by each of the above transfer methods?	Secure server/storage, encrypted and password protected. Users managed through active directory	
8.8	What measures are in place to ensure the security of information at rest? (This question applies to all information, whether in paper and/or electronic format)	Secure server/storage, encrypted and password protected. Users managed through active directory	
8.9	How will staff (RD&E and data processor staff) operating in this project be informed of their obligations under data protection/confidentiality law? *(all staff should do mandatory training, is their additional specific guidance?)*	Information Governance and Datix Training, info on the Hub, policies	
8.10	What practical training and guidance will staff operating in this project receive to ensure that they mitigate the risks of accidental loss, damage and destruction of information through human error? *(Mandatory IG training does not cover this, SOPs, systems training should cover this element)*	Datix training, users will not be able to delete. Datix administration overseen by Datix Certified professionals	
8.11	Have you completed all relevant IG and Security documents? - System Level Security Policy - Risk assessment - System BCP or Service BCP - Data Flow mapping - Access Control documentation (if required) - Cloud Questionnaire (if required) *(Please provide a copy with your DPIA submission)*	Yes - system level SLSP, Service BCPs (system BCP covered by contract)	

9	**Overseas Transfers**	**Response**	**ISF Feedback**
9.1	Are you transferring any personal and / or sensitive data to a country outside the United Kingdom? (Please list all destination countries)	Yes - Login (employee login username and email address) cache data of users is in Amsterdam All patient details, description of incident etc hosted in UK and not shared or mirrored overseas UK and Holland	
9.2	Has the IG team checked that the non UK country has an adequate level of protection for data security?	Yes	
9.3	Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?	AES-256 encryption	

10	**Further Information**	**Response**	**ISF Feedback**
10	Please provide any further information about your management of privacy risks that you have identified, which are unique to this project	Log ins will now work through adding users to active directory account and therefore users will automatically removed alongside leavers. Access to relevant information only will be set by a series of user profiles ensuring only relevant users get to see information that their role dictates .	

Data from	Data to	Master data set	Data Fields (Inc PID)	Transfer method	Risks ref	Internal/External	Contract/DSA (external only)	Approved by
PAS	*CDM*	*PAS*	*patient personal and health data*	*internal interface*	*Risk 1*	*Internal*	*n/a*	*Example*
				Via connector called Centrify connect https://docs.centrify.com/Content/CoreServices/Connector/ConnInstall.htm You install the Centrify Connector to integrate your Active Directory/LDAP service with Privileged Access Service. The connector allows you to, among other things, specify groups whose members can register and manage devices. It also monitors Active Directory/LDAP for group policy changes, which it sends to Privileged Access Service to update registered devices.				
Active Directory	DCIQ	AD	Username, Password, Name Email Address.		15		Contract signed with Datix	
DCIQ	NRLS	DCIQ	No PID information, category, subcategory, harm, description of incident	Download to XML and import to password protected NRLS website on weekly basis. No direct link	Linked via incident DPIA			
DCIQ	K041	DCIQ	No PID, subjects, sub subjects, age range of patient effected, type of staff member involved by mapped jobs	Download to excel and import to password protected K041 website on quality basis. No direct link	Linked via Feedback DPIA			

Cloud considerations

This section only requires completing if you are planning to store data in the Cloud. You may need to involve IT and / or the proposed system provider in completing this section.

Cloud criteria	Detailed answer
Why are you looking at Cloud solutions and not an in-house solution? Has an in-house solution been investigated?	Improved reporting capability, national reporting requirements
Will clinical data be hosted within the Cloud application?	Yes - incident, complaint and claim data related to
Is the Cloud data hosting service within the European Economic Area (i.e. the European Union or Norway, Iceland Lichtenstein)?	Yes
If 'No' to the previous question, does the country in which it is being hosted have adequate protection for the rights and freedoms of data subjects, as defined by the European Commission? (Further information is available on p.12 of the following document http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf. NB The US Safe Harbor agreement is no longer considered adequate, and has been replaced by the Privacy Shield, which went live on 01/08/2016. It is appropriate to answer N/A to this question if the Cloud data is hosted within the EEA.)	N/A
Is the Cloud service provider hosted on HSCN or the internet?	
What happens to the data in the event of the Cloud provider's business closure / insolvency?	
Have Finance been asked to perform a credit check regarding the Cloud service provider? What was the outcome? If not, why not?	Would this been completed with original purchase or mortality module which was done through
What arrangements would there be in place at the end of the contract with the Cloud service provider to transfer the data? Would there be any associated costs incurred by the Trust?	On-going licence fee
Who would legally own any data uploaded to the Cloud application by the Trust or its staff?	
Who, other than Trust staff, would have access to the data that has been uploaded to the Cloud application?	Datix technical support if required
Does the provider have other NHS contracts, and have you spoken to these organisations as part of due diligence? Please give full details.	Yes
What security frameworks and policies are in place by the Cloud service provider? Please direct the reviewer to them online, or embed copies here.	
What safeguards does the Cloud service provider have in place / offer to protect against Cyber Security attacks? Please direct the reviewer to documents online, or embed copies here.	
Will the transit of data between the Trust and the Cloud service provider be secure, e.g. by use of https?	