NHS
Royal Devon
University Healthcare
NHS Foundation Trust

Title: Imprivata Software

Reference Number: RDF1159-22
Date of Response: 27/01/23

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

1. *Please provide a copy of any Data Protection Impact Assessment conducted by yourself or any predecessor Trust into the use of Imprivata OneSign - Single Sign-On or related software applications provided by Imprivata.*
   Answer: Please find the Data Protection Impact Assessment attached, the Trust has redacted information that exempts disclosure under the Freedom of Information Act.

   The Trust cannot provide the 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.

Personal Information, where disclosure may contravene the Data Protection Act 2018 and therefore applies an exemption under Section 40 (2) - Personal Information of the Freedom of Information Act 2000 and Section 10 of the Data Protection Act 2018. The Trust only releases the names of Heads of departments.

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

Version: 2 **Updated Jan 2020**

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.

If you need further information please contact the Information Governance Office on [redacted]

Tab	Requirements	Useful links
Project Details	This page will be published on the website, please ensure you complete fully to explain tot the public what the project is doing and why personal data is required to be processed.	[redacted]
Assessment	This is the questions to understand how you are compliant with the GDPR and Data Protection Act 2018. Please provide as much detail as possible, if it is useful to break the data out you can use more than 1 column.	https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
Information Asset Register	The Information Asset Register must be populated with all new Information Assets or updated where the asset already exists.	[redacted]
Risk Assessment	This must be completed, more guidance is available in the Risk Assessment Policy and Procedure on the Hub	
Additional Documents	Please ensure you provide the relevant documents or include within this page	
Outcome	The first section will be completed by IG when the DPIA goes through the relevant forums for approval. If you speak to anyone in IG or IT for advice you may wish to record their feedback here in the second section.	

Name of Proposal Project Manager	[redacted]
Job Title of Project Manager	[redacted]
Phone number of Project Manager	[redacted]
Email of Project Manager	[redacted]

DPIA Completed by	[redacted]
Job Title	[redacted]
Email Address	[redacted]

Senior Staff Members/Committees endorsing this project	[redacted]

Royal Devon & Exeter NHS Foundation Trust

Data Protection Impact Assessment Toolkit Version 2

DPIA Reference	DPIA1135
DPIA Title	Imprivata OneSign - Single Sign-On
Summary of Proposal	Imprivata OneSign® Single Sign On (SSO) is what we intend to use to address identity management security and user authentication challenges. OneSign is an appliance-based approach that requires no other software or hardware to deploy and maintain, where no changes to existing code or directories is required. Imprivata affects staff data in relation to accessing systems.
Date Ratified	21 July 2020

1	Summary of Processing Activity	Response	ISF Feedback
1.1	Will identifiable personal data be processed as part of this project?	Yes	
1.2	Will any of the following "special categories" of personal data be processed as part of this project: • 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	No	
1.3	Please list the data elements (for 1.1 and 1.2) that will be used as part of this project (e.g.; name, address, national insurance number, medical diagnosis and treatment details, etc.)	[redacted].	
1.4	Please categorise who the information is about (e.g.; dialysis patients, medical staff, etc.)	[redacted]	
1.5	Please justify why it is necessary for this personal data to be processed	The Imprivata solution simplifies password management and authentication. A username needs to be entered in order to apply the correct user credentials for the systems Imprivata will log in for the user.	
1.6	Please describe how this information will be obtained and who from	The information will either be automatically pulled into Imprivata when a user logs into a connected system for the first time or by the user themselves, selecting the system and entering the correct credentials	
1.7	Please describe how/where this information will be stored	[redacted]	
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.)	Only the individual entering the credentials will be able to process them.	

1.9	Please describe all third party organisations that this information will be shared with, what data will be shared and why	No third party organisation will have this information shared	
1.10	Does this project require the installation of new software?	Yes	
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.	No, [redacted].	

2	Fairness, Transparency and Lawful Bases	Response	ISF Feedback
2.1	How will data subjects be told about how their personal data will be used as part of this project? Where is the fair processing notice located?	Included in staff privacy notice. Staff will also be informed using standard communication methods when rolling out projects i.e. RDE Hub Must read, and email communications to staff	
2.2	What lawful basis is the Trust relying upon to process this personal data for this project?	6(1)(e) – Official authority	
2.3	If processing special categories of personal data for this project, what further lawful basis is the Trust relying upon?	No special categories processed	

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.	Access control, so cannot be anonymised	
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	[redacted].	

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?	[redacted]	
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	[redacted].	

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?		
6.3	How will the data be destroyed at the end of its retention period?		

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?	[redacted]	
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?	[redacted]	
7.3	Do you intend to send direct marketing messages by electronic means? This includes both live and prerecorded 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?	[redacted]	
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?	No	
7.7	What procedures are in place for the rectifying / blocking / erasure / destruction of data by individual request or court order?	[redacted] [redacted].	

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?	No	
8.2	If 'yes', does the contract with the data processor contain all of the necessary Trust Information Governance clauses?	N/A	

8.3	Has the data processor registered as a data controller with the Information Commissioner's Office?	N/A	
8.4	If 'yes', what is their registration number?	N/A	
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)	[redacted].	
8.6	By what method(s) will information be transferred?	No data is transferred in or out of the system	
8.7	What measures are in place to ensure the security of information being transferred by each of the above transfer methods?	N/A	
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)	[redacted].	
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?	Weekly project delivery team meetings	
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?	Training has been provided by the supplier.	
8.11	Is there a System Level Security Policy in place? (Please provide a copy with your DPIA submission)	[redacted]	
8.12	Has an information risk assessment been carried out and reported to the Information Asset Owner? (Please provide a copy with your DPIA submission)	See risk assessment tab	
8.13	Is there a contingency plan or backup policy in place to manage the effect of an unforeseen event? (Please provide a copy with your PIA submission)	[redacted].	

8.14	Are there documented procedures in place to recover data (both electronic / paper) which maybe damaged through: • Human error • Computer virus • Network failure • Theft • Fire • Flood • Other disaster (Please provide a copy with your PIA submission)	[redacted]	

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)	No	
9.2	Has the IG team checked that the non UK country has an adequate level of protection for data security?	N/A	
9.3	Are measures in place to mitigate risks and ensure an adequate level of security when the data is transferred to this country?	N/A	

10	Further Information	Response	ISF Feedback
10.1	Please provide any further information about your management of privacy risks that you have identified, which are unique to this project		

Please complete Information Asset Register details in full on this form

If your project relates to an information asset which has already been registered on the Information Asset Register, please contact the IG Team for the current register details

Please note that full, accurate and up-to-date information must be completed on this form, regardless of whether this project relates to a new or already registered asset

If you need to register/amend register details for more than 1 information asset, please duplicate this tab and complete for each asset

	Response
Reference *IG Team will generate this*	[redacted]
Name of Information Asset	[redacted]

Description of Information Held /Components of Asset *Is the asset made up of different components, such as different system modules or - if paper-based - a combination of different documents/records?*	[redacted]
Processing Personal Data? *Answer "Yes" if your information asset processes any information which could identify a living person.*	[redacted]
Personal Data Items Held *Please list these, separated by a semi-colon; e.g., "Name; address; date of birth; NHS number; medical diagnosis; treatment details", etc.*	[redacted]
Purpose of Asset *What purpose is the information used for?*	[redacted]
Media *Paper or electronic?*	[redacted]
Location *If electronic; must include full network location or system name. If an information system, please include where the data is hosted (whether on-site/elsewhere).* *If paper; must include building, room and location within room.* *Must be descriptive enough that anyone could find the information from this description.*	[redacted]
Priority *This is the priority level of the system.*	[redacted]
Information Asset Owner (IAO)	[redacted]
IAO Job Title	[redacted]
IAO Email Address	[redacted]
Information Asset Administrator	[redacted]
Division	[redacted]
Area	[redacted]
Retention Period *After what period will the information be destroyed?*	[redacted]
How will the information be destroyed?	[redacted]
Current Business Continuity Plan (BCP) Date	[redacted]
Most Recent BCP Test Date	[redacted]
Current System Level Security Policy Date	[redacted]
Current Risk Assessment Date	[redacted]
Most recent IAO Training Date	[redacted]
Who has access? [redacted]	[redacted]
What controls are in place to restrict access to only those individuals who are authorised to access it? [redacted]	[redacted]
Audit Trail? *To what extent can you find out who has accessed the information? Is there an audit trail available?*	[redacted]

Is the information backed-up? If so, how? [redacted] [redacted]	[redacted]
System linkages *Does the system automatically send/receive data from other systems? List all such systems*	[redacted]
Article 6 Condition for Processing *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".* [redacted]	[redacted]
Processing Special Categories of Personal Data? *'Special Categories' are information about:* *• 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* *Answer "Yes", if your information asset processes one or more of the above*	[redacted]
Article 9 Condition for Processing *If the processing of the information in this information asset is necessary for delivering healthcare/treatment, answer "9(2)(h) Health and Social Care...".* [redacted]	[redacted]
DPIAs *If a Data Protection Impact Assessment (including this one) has been undertaken in respect of this asset, please include the reference number(s) here*	[redacted]

No	Hazard and Raw Score			Risk Description and Effect Consider the use of personal / sensitive data, whether it is on computers or paper, and any potential risk there may be of / from: - Accidental loss, - Unlawful destruction, - Unauthorised alteration, - Unauthorised disclosure, - Unauthorised access,	Control Measures in Place What physical, personnel, technical and policy or procedural controls are already in place to mitigate the risks?	Current Risk Rating			Action Plans/Further Controls What additional physical, personnel, technical and policy or procedural controls are you developing to mitigate the risks?	Target Risk Rating		
	L	C	RR			L	C	RR		L	C	RR

				- Unauthorised sharing, - Physical damage, - Cyber security incidents, - Poor practice, - Inadequate training								
				REDACTED								
				REDACTED								
				REDACTED								
				REDACTED								
				REDACTED								
				REDACTED								
				REDACTED								
				REDACTED								
				REDACTED								
				REDACTED								
				REDACTED								
				REDACTED								
				REDACTED								

Business Continuity Plan	
Which BCP is this DPIA related to? Either department or System BCP, either provide the reference or a copy of the updated BCP to reflect this new information asset.	
Service Level Security Plan	
Please provide a copy of the SLSP, or reference to it for all systems.	
Access Control	
Please ensure you have provided detail on Access control here if not already elsewhere in the documentation or attach a separate document with relevant details	
Data Flow mapping	
Please include or provide a copy of the data flow mapping	
Cloud Based Projects	
Please complete the Cloud base projects template and include within this DPIA or as an attached document.	

Date Reviewed	Outcome	Comment
19/05/2020	Approved	[redacted]

Date Reviewed	Outcome	Comment