Royal Devon University Healthcare NHS Foundation Trust

Limbus AI

Reference Number: RDF1454-23
Date of Response: 03/05/2023

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

Please be aware that the Royal Devon University Healthcare NHS Foundation Trust (Royal Devon) has existed since 1st April 2022 following the integration of the Northern Devon Healthcare NHS Trust (known as Northern Services) and the Royal Devon and Exeter NHS Foundation Trust (known as Eastern Services).

I understand that your Trust is a user of the Limbus AI (https://gbr01.safelinks.protection.outlook.com/?url=https%3A%2F%2Flimbus.ai%2F&data=05%7C01%7Crduh.foi%40nhs.net%7C3b1e638f1a284262a69d08db40db4faa%7C37c354b285b047f5b22207b48d774ee3%7C0%7C0%7C638175082896277284%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C3000%7C%7C%7C&sdata=yGqwL0ShinZ4efs9%2FDcBdlYcoJBYRN8NWImXzxMPgAA%3D&reserved=0) contouring app for radiotherapy.

1. Please provide a copy of any Data Protection Impact Assessment conducted overuse of this application. Please find attached redacted Data Impact Assessment.

The assessment has been redacted as 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 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. 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.

2. Does your Trust share back any anonymised/ pseudonymised usage data from the app to the supplier? No. We do not routinely share any data with Limbus AI.

3. If so, please provide a copy of any agreement relating to that data flow. This question Is not applicable.

Royal Devon & Exeter NHS Foundation Trust
Data Protection Impact Assessment Toolkit **Version 0.1**

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.

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

DPIA Reference	DPIA1132
DPIA Title	Limbus Contour
Summary of Proposal	To install, for a trial period of 2 - 6 months, Limbus Contour auto-segmentation software. This utilises machine learning to auto-contour anatomical structures on CT datasets in preparation for radiotherapy. This will reduce the time required to manually contour these structures providing efficiency and resource savings. Potentially, this could provide benefits in terms of capacity and staffing resources, freeing-up clinician time as well as physics and radiotherapy staff.

Name of Proposal Project Manager	[redacted]
Job Title of Project Manager	Principal Dosimetrist
Phone number of Project Manager	402155
Email of Project Manager	[redacted]

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

Senior Staff Members/Committees endorsing this project	[redacted]

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	Yes	*Does this include medical images and therefore health data?In which case this should be yes.* *Corrected to Yes -medical images processed.*
1.3	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.)	DICOM (Digital Imaging and Communications in Medicine) tag information embedded in medical imaging datasets: Typical details would include, patient name, D.O.B., hospital number, institution, referring physician. A full list of tags can be found here: https://www.dicomlibrary.com/dicom/dicom-tags/. Not all fields would have information, depending on what imaging device is used and what data staff input.	
1.4	Please categorise who the information is about (e.g.; dialysis patients, medical staff, etc.)	Radiotherapy patients Medical staff Institution details	
1.5	Please justify why it is necessary for this personal data to be processed	Information is embedded in the file data of imaging datasets. Correct patient identification is essential for patient safety, to ensure that imaging data and diagnostic information corresponds to the relevant patient undergoing radiotherapy treatment.	
1.6	Please describe how this information will be obtained and who from	Embedded data in image datasets conforming to the DICOM international standard: https://www.dicomstandard.org/ Data comes from medical imaging devices (e.g. CT scanners, etc).	
1.7	Please describe how/where this information will be stored	Data will be stored on the secure Trust network drive.	*Information to be stored in shared network drive for the duration of the trial.* *Happy to comply with this.*
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.)	Radiographers and Medical Physics staff. In terms of patient identifiable data, only viewing is required.	
1.9	Please describe all third party organisations that this information will be shared with, what data will be shared and why	None.	
1.10	Does this project require the installation of new software?	Yes. Limbus Contour (Limbus AI Inc.) application to be installed on a local client PC: https://limbus.ai/	
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. Currently image datasets pass directly from the CT scanner in the Radiotherapy Department to a network share folder, before being imported to the treatment planning system (Varian Eclipse TPS version 15.6). The new software would be an intermediate step in the process between the CT scanner and share folder.	

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?	No change to the existing embedded DICOM metadata. The auto-segmentation software does not alter this information, or use it for anything other than patient identification.	
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?	9(2)(h) – health and social care (including occupational health)	

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. Informed consent for Radiotherapy given. Data collection does not vary from current standards, with patient identification data (DICOM) required as for all current patients requiring External Beam Radiotherapy planning. Adheres to patient identification and privacy principles as documented in Confidentiality: NHS Code of Practice (2003) and the Manual for Cancer Services: Radiotherapy Measures, version 5.0 (2013).	
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 for patient identification only.	
4.2	Has the use of anonymous data been explored? If so explain why this is not viable.	No, see 3.1 above: Identification of patient imaging data is vital for the safe and effective provision of Radiotherapy.	
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	Evaluation software complies with DICOM standard. Since datasets will be stored on the hard drive of a local Trust client PC during the evaluation period, then the data is protected to current IT standards. Installation of software already agreed in principle pending the approval of this DPIA application (Non Standard Software Request Form - IT Service Desk Ticket no. [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?	No. Application displays DICOM patient information, it is not necessary to edit the data.	
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	Data is collected at source (CT scanner) following standard processes.	

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?	Evaluation period will last 2 - 6 months.	
6.3	How will the data be destroyed at the end of its retention period?	Via consultation with IT: Data on local hard drive can be securely erased if necessary.	

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? How will IG have access?	Access requests can follow the standard IG process.	*Will IG have access to this data direct or through medical records? If not who is the contact for IG to go to for requests for this? Contacts are [redacted]. The data will be on a network share, the application will be installed on a client PC in the Radiotherapy planning room [redacted]. If direct access is required, then IT would be able to arrange this via a Remote Desktop Connection if desired.*
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?	DICOM data is collected and stored as per standard processes. Medical images from the Radiotherapy CT scanner are available on the PACS system. Additional DICOM data for Radiotherapy purposes is stored in the Varian ARIA patient management system.	
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?	Data is confidential and not released for direct marketing purposes.	
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?	Data stored as stated in Section 7.2	

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)	At the Treatment Planning System end of the process, there is an electronic log that captures user interactions (via secure username/password combination) as part of the Patient Management System (Varian ARIA version 15.1). This is not necessarily a function of the auto-segmentation software (Limbus Contour).	
8.6	By what method(s) will information be transferred?	DICOM standard.	
8.7	What measures are in place to ensure the security of information being transferred by each of the above transfer methods?	IT network security protocols.	
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)	All applications require Trust login via secure username/password combination.	
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?	Only Trust staff with Information Governance mandatory training will have access to the system, as listed in Section 1.8	*How will this be checked and managed?* *Secure Trust login for the client PC, and username/password combination for the application.*
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?	Only specialised radiotherapy planning staff as listed in Section 1.8 will have access to the system. These staff are state registered professionals (HCPC and IPEM) who have received training and adhere to professional codes of conduct. They have all received mandatory Trust Information Governance training.	
8.11	Is there a System Level Security Policy in place? (Please provide a copy with your DPIA submission)	Information Governance Policy Data Protection Policy	
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)	Non Standard Software Request Form.	*Needs amending to read Minimum Windows XP but compatible with all Microsoft operating systems.* *Amended entry on Non-standard Software Request Form.*
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)	Backup storage.	
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)	No processes documented, but training provided for select staff. CT scanner datasets are backed-up to the Trust PACS system, and can be retrieved from there by staff members with access to PACS (for which they have received Trust provided training). Imaging datasets and ancillary information lost from ARIA/Eclipse can be retrieved from the system backup which is overseen by Varian and Trust IT department.	

9	Overseas Transfers	Response	ISF Feedback
9.1	Are you transferring any personal and / or sensitive data to a country outside the European Economic Area? (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	Patient identification via DICOM metadata is a worldwide safety standard. The current radiotherapy planning process requires the export of imaging data from the CT scanner in the Radiotherapy Department to the Treatment Planning System. Checks are performed to ensure the exported CT data is imported to the correct, corresponding patient data in the TPS. The auto-segmentation software will be an intermediate step in the current process and will follow the same checks.	

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*	
Name of Information Asset	Limbus Contour
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?*	Single application
Processing Personal Data? *Answer "Yes" if your information asset processes any information which could identify a living person.*	Yes
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.*	Name; patient sex; date of birth; hospital number.
Purpose of Asset *What purpose is the information used for?*	Patient identification for safety reasons.
Media *Paper or electronic?*	Electronic
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.*	Trust network share drive
Priority *This is the priority level of the system.*	[redacted]
Informaton Asset Owner (IAO)	[redacted]
IAO Job Title	Head of Radiotherapy Physics
IAO Email Address	[redacted]
Information Asset Administrator	External Beam Planning
Division	Cancer Services

Area	Radiotherapy
Retention Period *After what period will the information be destroyed?*	At end of trial period (2 - 6 months).
How will the information be destroyed?	Securely erased from network share drive
Current Business Continuity Plan (BCP) Date	29-Jan-20
Most Recent BCP Test Date	
Current System Level Security Policy Date	29-Jan-20
Current Risk Assessment Date	29-Jan-20
Most recent IAO Training Date	
Who has access? *State if the information is accessible to a named individual(s), team(s), anyone in the Trust, publicly available, etc.*	Medical physics staff and radiographers.
What controls are in place to restrict access to only those individuals who are authorised to access it? *Examples include; "record stored in locked filing cabinet", "password protected", "unique username and password required to log-in", "located in network drive with restricted access"; etc.*	Client PC is in Treatment Planning room, which is occupied during the day and locked at night. PC is on secure hospital network. Secure Trust login required to access system, application protected with unique username/password combination.
Audit Trail? *To what extent can you find out who has accessed the information? Is there an audit trail available?*	See Section 8.5
Is the information backed-up? If so, how? *Backing-up means a copy of files is automatically saved on a regular basis, so if the original is destroyed or damaged a recent copy is located elsewhere. This applies to electronic records only.* *All files stored on RD&E shared network drives are automatically backed up by the IT department on a daily basis. No master electronic files should be stored on local drives i.e. the C drive of a PC or laptop as these files are not backed up. If the hard drive of a PC or laptop fails files stored on the drive will be lost or corrupted.*	See Sections 8.13 and 8.14
System linkages *Does the system automatically send/receive data from other systems? List all such systems*	No, but would operate in this manner if purchased.
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". If not, or you are unsure, call the Information Governance Team on x2235.*	6(1)(e) – Official authority

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*	No
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...". If not, or you are unsure, call the Information Governance Team on x2235.*	9(2)(h) – health and social care (including occupational health)
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*	This one (haven't received a reference no. yet)

Name of Forum	Date Reviewed	Outcome	Comment
Information Security Forum	24/06/2020 and 20/08/2020	Approved	Needs response to questions on Assessment. Needs to be stored on network drive for trial. Needs to have a risk assessment. If completed and resubmitted by COP 30th June can be reassessed at Caldicott meeting for approval to be ratified at IGSG in July. Further DPIA submitted for meeting on 20/08/2020. Approved for trial period and request made that if trial successful and system to be used on a permanent basis that the DPIA be amended and re-submitted.
Information Governance Steering Group	22/09/2020	Approved	Ratified