NHS
Royal United Hospitals Bath
NHS Foundation Trust

Data Protection Impact Assessments

Introduction

This Data Protection Impact Assessment (DPIA) has been completed by Royal United Hospitals Bath to assess the privacy risks associated with the COVID-19 Online Imaging Teaching Library. The Library holds fully anonymous copies of images of patients diagnosed with COVID-19. These images are uploaded by radiology departments in NHS Trusts and NHS Foundation Trusts throughout England.

We are providing this DPIA to Trusts that are intending to submit images to the Library, with the intention of informing their internal information governance approval processes. This DPIA has been reviewed and endorsed as fit for purpose by NHSX.

The Data Protection Impact Assessment (DPIA) must be completed whenever there is a change in an existing process or service, or new processes of an information asset is introduced that is likely to involve a new use or significantly changes the way in which personal data is handled.

The Data Protection Impact Assessment (DPIA) is a process which assists in identifying and minimising the privacy risks.

An effective DPIA is a tool (a Risk Assessment), to help identify the most effective way to comply with Data Protection obligations and meet individuals' expectations of privacy allowing the organisation to identify and resolve any problems at an early stage, reducing the associated costs and damage which might otherwise occur.

Privacy may be defined as:

- Physical privacy – the ability of an individual to maintain their own physical space.
- Informational privacy – the ability of a person to manage their information and its use.

Who is responsible for completing a DPIA?

The person who is responsible for introducing a new or revised service or changes to a new system, process or information asset is responsible for the completion of a DPIA.

The DPIA must be formally recorded and assigned by the project board or senior manager.

The Information Governance Lead/Trust Data Protection Officer (DPO) should be consulted at the start of the design phase of any new service, process, purchase or implementation of an information asset etc. so that they can advise on the need and procedures for completing the DPIA.

Contact Details: Graeme Temblett-Willis, Head of Information Governance/DPO
Email: ruh-tr.IGQueries@nhs.net
Tel: 01225 82 6268/4416

Data Protection Impact Assessment Tool

Please complete the initial screening questions to determine if a full Data Protection Impact Assessment (DPIA) is required:

Section 1: Initial Screening Questions		Response (Yes / No)
Identity Risk	1. Will the project process personally identifiable information? This is usually a name, NHS number or images; but could also be a combination of other data which could lead to identification such as address, DOB, hospital number, gender.	No
Data Risk	2. Will the project process special category data on a large scale? Special category data includes health data. Consider the number of data subjects concerned as a specific number or as a proportion of the relevant population; the range of different data items being processed; the duration; and the geographical location. Note: a clinician processing data about the patients that they provide direct care to would not be considered a large scale.	No
	3. Will special category data be used to make any decisions on access to services?	No
	4. Will the project involve the processing of genetic data?	No
	5. Will the project involve matching or combining datasets from different sources?	No
Technology Risk	6. Does the project involve using new technology, or extensively change or upgrade an existing process?	Yes
	7. Will the project include the processing of biometric data such as fingerprints, voice recognition or facial recognition?	No
Personal Risk	8. Will the project use automated profiling? e.g. data from web searches, cookies, browsing history, etc. used to build an identity	No
	9. Does the project involve collecting personal data from somewhere other than the data subject - without informing them or directing them to the Trust's privacy notice?	No
	10. If there was a breach of confidentiality, would this likely endanger the data subject's health or safety?	No
	11. Will the project involve tracking an individual's location or behaviour?	No
Organisation Risk	12. Does the project involve monitoring public places on a large scale? e.g. CCTV or automated number plate recognition (ANPR)	No
Children	13. Will the process profile children, or specifically target marketing or online services to them?	No

If Q1 was answered 'no', a full DPIA is not required. When personal information is not used, there is a significantly reduced risk to privacy. If Q1 was answered 'yes', see below.

If all answers for Q2 – Q13 were answered 'no', a full DPIA is not required. If any of the questions were answered 'yes', a full DPIA is required.

Section 2: Project details		
Project Name:	**BSTI COVID-19 Online Teaching Library**	
Project Lead Details -	Name:	Dr Graham Robinson
	Telephone number/ext.:	01225 821174
	Email address:	ROBINSON, Graham (ROYAL UNITED HOSPITALS BATH NHS FOUNDATION TRUST) <grobinson1@nhs.net>
The Controller(s) for the processing	The British Society for Thoracic Imaging (BSTI) and RUH Bath are jointly responsible for the processing of the anonymous images for the purposes of this project. As no personal data are to be processed, the processing falls outside the scope of data protection legislation, so the parties are not formally controllers – however the data will be processed under formal controls as described in this DPIA. BSTI is responsible for managing the uploading of images, and publishing of selected images to the published Teaching Library. RUH Bath is responsible for entering in to and managing the contract with Cimar UK Ltd. Individual Trusts are controllers for the processing to anonymise the images prior to uploading. This processing is outside the scope of this DPIA.	
Name of any organisations involved in the sharing of information:	Cimar UK Ltd (Medical Imaging Cloud Service) (processor for RUH Bath and BSTI)	
Background information on the project:	With the outbreak of the new COVID-19 virus, urgently providing a nationally accessible teaching resource for Radiologists to use is critical. The aim is to create an online anonymised teaching/training library containing example medical imaging of actual cases where Coronavirus has been detected in patients imaging.	
Benefits of the project:	The projects aim is to be used as an expert-led teaching resource to inform and guide radiologists nationally on the COVID-19 condition, and how to detect the virus in patients. Unrestricted public access to the anonymous images will provide an easily accessible training resource.	

Section 3: Data	
What types of data will be used? (Please tick)	☐ Personal Data ☐ Special Category Data ☐ Pseudonymised Data ☑ Anonymised data
Why is the data/information being used? What is the data (detail i.e. name, NHS# etc)?	Medical imaging (CT) of patients with known COVID-19 infection. Data provided to Cimar will be anonymised by submitting Trusts and will not contain any personal identifiers from the source. As an additional precaution, the automatic upload process removes any identifiers that may remain in the image. The data are uploaded

	and stored at UK Cloud (https://ukcloudhealth.com) with no identifiable metadata. No identifiable data will be used/stored/accessed outside of the sending Trusts network.
How is the data/information being collected?	Web-upload technology which automatically: Anonymises all images before upload (as a secondary measure to remove identifiers that may have been missed by the Trust). Compresses all images before transit Transmits the above over HTTPS/TLS1.3 encrypted connection
How many data subjects, such as patients or staff, are or will be affected?	Unknown – an estimation of circa 500 patient cases may be used/stored in the online library, however an exact number can only be estimated at this time.
Where is the data/information going to be held?	All data will be hosted at https://cloud.Cimar.co.uk - a Cloud PACS which is physically hosted at https://ukcloudhealth.com/ and in the UK only.
How is the data/information stored and for how long?	All imaging data will be stored in an encrypted database with no identifiable meta-data whatsoever. Data will be stored for a Year or longer depending on the clinical need for access to it as a training resource.
Is there an electronic system used to collect / record / process the data?	Yes – Cimar's cloud technology includes zero-footprint web-upload, compression and encryption utilities. This is accessed via secure links (URLs)
How is the data/information going to be kept secure?	All access to the master anonymised data sets will be by RBA (Role Based Access) secure login. Only the BSTI Committee have access to the holding bay and the main database. The Teaching Library is available to the radiologists and the general public via the BSTI web site.
How is the quality of the data collected going to be checked?	The BSTI Committee vets the images in a holding bay before inclusion in the main database. The Committee is also responsible for selecting appropriate images for publication to the Teaching Library. All uploaded cases proceed through an approval process and can only be passed to general teaching access after clinical oversight and preparation has first been applied by a limited number of administrative sub-specialty clinicians of the BSTI Committee.
Where/how will any data quality issues be addressed/resolved?	A record of quality issue will be addressed and corrected online in a master worklist with no access other than by pre-registered administrator users.
Section 4: Processing Information	
What is the frequency of data sharing?	Trusts are free to upload images as an when required. Access by Radiologists other health professionals and the general public nationally and globally.

<table>
<tr><td>Is the data to be held in a Cloud based system?</td><td colspan="3">Yes – cloud.cimar.co.uk is the main host. The specific library access is https://bsticovid19.cimar.co.uk/</td></tr>
<tr><td>How is the information accessed?</td><td colspan="3">By BSTI administrators – only via pre-registered login access with strong (forced renewable) passwords. 2FA access can be turned on if required.
The published teaching library will be available to anyone without prior authorisation or logon credentials.</td></tr>
<tr><td>How is access managed/controlled? E.g. audit trails and/or security?</td><td colspan="3">All access requiring login credentials is audited and captured.
All administrator users are role based only with tightly configured functionality permission constraints
Thorough audit trails are available at all times to administrator users.</td></tr>
<tr><td>Describe the flow of information and the organisation(s)' roles e.g. data controller/processor. (include a flow diagram if appropriate)</td><td colspan="3">The organisations responsible for processing the data will the British Society for Thoracic Imaging and RUH Bath once the data has been uploaded. Any organisation submitting an imaging case/study for inclusion into the library will provide only anonymised data as defined by the GDPR.
The Processor is Cimar UK Ltd.
The anonymous images will be shared by the admin to the published library where it will be available for general Radiologist access (public access) as a teaching resource.
NHSX has been consulted in this process and has endorsed the project to enable further learning of COVID-19 at the earliest opportunity and benefit of the public.</td></tr>
<tr><td>Is any data being sent outside of the EU?</td><td>No</td><td><b>If yes</b>, which country is the data information being sent to?</td><td></td></tr>
<tr><td>Is there an information sharing agreement /protocol/contract with the external organisation?</td><td colspan="3">There is a data processing agreement in place between RUH Bath and Cimar UK Ltd. for the processing of the data.
A contract is in place between Cimar and BSTI recognised as a special interest group by the RCR.</td></tr>
<tr><td>How long will the data be used for?</td><td colspan="3">For as long as the RCR deem it necessary and beneficial. On notification to delete data, Cimar can implement purge rules in the cloud to completely remove all records permanently from Cloud storage.</td></tr>
<tr><td>How will the data be deleted when no longer required?</td><td colspan="3">Automated Purge rules in the cloud will scrub all data meeting rules criteria from all storage points. In addition, administrators are able to delete one or many records individually or in bulk, at any time</td></tr>
<tr><td>Who is monitoring / responsible for this flow of information?</td><td colspan="3">(Detail Asset Register number / Data flow reference obtained on completion from IG Team)
Ruh Asset register #12/2020
Data Flow register # 331/2020</td></tr>
</table>

Section 5: Legal Basis

<table>
<tr><td>For what purpose/legal basis is it proposed to use this data / information?</td><td colspan="4">Article 6 GDPR: Not applicable – the data are not personal data so not captured by GDPR
☐ Public Task
☐ Consent
☐ Contract
☐ Vital Interests
☐ Legal Obligation
☐ Legitimate Interests
If legitimate interests basis, state why the processing is necessary and justify it against the individual’s right to privacy’
Please click on the wording below when processing Special Category (health) data:
Article 9 GDPR
Not applicable.</td></tr>
<tr><td rowspan="2">Are the data subjects (e.g. patients/staff) informed about this new processing of information?</td><td rowspan="2">No the data is truly anonymised in accordance with ICO Guidance</td><td colspan="3">How are the individuals informed?</td></tr>
<tr><td colspan="3">N/A</td></tr>
<tr><td>Is the processing of information in the Trust’s Privacy Notice</td><td>Not applicable</td><td colspan="3"></td></tr>
<tr><td>Is there an option for the data subject to opt out of their information being shared or accessed?</td><td colspan="4">No</td></tr>
<tr><td rowspan="2">Can data subjects request copies of their information?</td><td colspan="4">If yes, please detail how they would do this?</td></tr>
<tr><td colspan="4">All data will be deliberately de-identified and anonymised by submitting Trusts before being uploaded to the Library therefore cannot be re-patriated with its originating subject.</td></tr>
<tr><td>Name of person(s) completing this DPIA</td><td colspan="2">Howard Jenkinson</td><td>Date</td><td>04 Mar 2020</td></tr>
<tr><td>Data Protection Officer - Review of DPIA</td><td colspan="2">Graeme Temblett-Willis</td><td>Date</td><td>09/03/2020</td></tr>
</table>

Note: **Special Category Data:** is more sensitive, and so needs more protection. This includes personal data, revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.

Lifecycle of the DPIA
Draft created 04/03/2020 completed by CIMAR UK Ltd Final authorised by RUH Bath DPO 05/03/2020 appropriate registers updated, copy provided to radiology and CIMAR UK Ltd for records and auditing purposes. Version 2 updated to reflect use of Hospital # at Trust level only 09/03/2020. Version 3 updated to reflect additional detail of no identifiable data and data controller responsibilities 24/03/2020. Version 4 final version for dissemination.

Privacy Risk Assessment:

Use the table which follows to record privacy risks identified when completing the DPIA. The following table is a guide to the scores to be used for likelihood and consequence.

The overall risk rating reflects both the likelihood that harm or loss will occur and the severity of its outcome: **(i.e. risk = likelihood x consequence).**

Risk Assessment Matrix						
Consequence	Catastrophic **5**	5	10	15	20	25
	Major **4**	4	8	12	16	20
	Moderate **3**	3	6	9	12	15
	Minor **2**	2	4	6	8	10
	Negligible **1**	1	2	3	4	5
		Rare 1	**Unlikely 2**	**Possible 3**	**Likely 4**	**Certain 5**
	Likelihood					

Privacy Risks identified following completion of DPIA				
Risk	**Score (L x C)***	**Mitigating Actions**	**Score (L x C)***	**Date of Review**
Transferring of data outside of the EEA Non-compliance:- No adequacy arrangement results in serious non-compliance with the data protection legislation. This faces regulatory action and exposes the vulnerability of an organisation as it is a breach. If consequently there is any loss of personal data to non-trusted sources this is a further breach and risks privacy re onward sharing of personal data; reputational damage; loss of trust by data subjects.	N/A	The data are held in UK on UKCloud – an established platform for the NHS.	N/A	25/03/2020
Misuse of information by those with access	1*3 = 3	• Images are anonymous • BSTI access authorisation process for access to the database	1*3	25/03/2020
Adequate data processing agreements with relevant data processors;	1*3	• No personal data are to be processed by CIMAR so GDPR does not require a data processing agreement. • BUH has in place an agreement with CIMAR to govern the processing.	1*3	25/03/2020
Lack of technical or organisational measures implemented to ensure appropriate security of the personal data	1*3	• Web-upload technology (see below) • BSTI access authorisation process.	1*3	25/03/2020

Personal data not being encrypted both/either in transit or at rest	1*3	• Web-upload technology which automatically: • Anonymises all images before upload. • Compresses all images before transit • Transmits the above over HTTPS/TLS1.3 encrypted connection	1*3	25/03/2020
Risk of images being upload inappropriately	1*3	The BSTI Committee vets the images in a holding bay before inclusion in the main database.	1*3	25/03/2020

∗ **Likelihood (L) x Consequence (C)**