Data Protection Impact Assessments

Introduction

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 <u>all</u> 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>
Name of any organisations involved in the sharing of information:	Cimar UK Ltd (Medical Imaging Cloud Service)	
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 Corono Virus 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.	

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 will include the unique hospital number **not** the NHS number. The hospital ID allows for previous and current imaging to be identified and amalgamated as related studies. This number is released externally from the respective Trust or healthcare provider as it is to assist in the measure of patients affected by the virus. It should be noted that this number will be not viewable in any publicly viewed training images. All imaging is then anonymized automatically at upload 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. 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 estimaol9ted at this time

Where is the data/information going to be held?	The data holding the Hospital number will be retained by each individual Trust andQA not released further. All data will be hosted (anonymised) 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 anonymised and split (PHI will be stored in an encrypted database – all imaging will be stored in S3 storage with no identifiable meta-data whatsoever. Data will be stored for perhaps 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 (ULRs)
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. As a teaching resource, completed cases will be available directly through a login via the RCR or NHS England websites for example
How is the quality of the data collected going to be checked?	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.
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?	Potentially, very wide access to Radiologists nationally. Users may re-visit teaching and illustrative material and cases, multiple times.
Is the data to be held in a Cloud based system?	Yes – cloud.cimar.co.uk is the main host. The specific library access is https://bsticovid19.cimar.co.uk/
How is the information accessed?	By administrators – only via pre-registered login access with strong (forced renewable) passwords. 2FA access can be turned on if required. General Radiologist access to the published teaching library will be able to access without logon.
How is access managed/controlled? E.g. audit trails and/or security?	All access is audited and captured. All users are role based only (with tightly configured functionality permission constraints Thorough audit trails are available at all times to administrator users.
Describe the flow of information and the organisation(s)' roles e.g. data controller/processor. (include a flow diagram if appropriate)	The data controller will be any organisation submitting an imaging case/study for inclusion into the library. The cloud-account administrator will vet the anonymised imaging for suitability, and if acceptable will add annotations and teaching material in support of the case. Once complete and ready to publish, the case/study will be shared by the admin to the published library where it will be available for general Radiologist access as a teaching resource.

Is any data being sent outside of the EU?	No	**If yes**, which country is the data information being sent to?	
Is there an information sharing agreement /protocol/contract with the external organisation?	Provision of technology for the use by this teaching service is provided "as is" at no cost by Cimar UK. As all data is fully anonymised at all times, it is regarded as being safe to share without formal ISA's.		
How long will the data be used for?	For as long as the RCR and NHS England 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.		
How will the data be deleted when no longer required?	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		
Who is monitoring / responsible for this flow of information?	(Detail Asset Register number / Data flow reference obtained on completion from IG Team) Ruh Asset register #12/2020 Data Flow register # 331/2020		

Section 5: Legal Basis

For what purpose/legal basis is it proposed to use this data / information?	Article 6 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 Medical diagnosis/health and social care	
Are the data subjects (e.g. patients/staff) informed about this new processing of information?	No the data is truly anonymised in accordance with ICO Guidance	How are the individuals informed? N/A

Is the processing of information in the Trust's Privacy Notice	Yes	Please review the Trust's Privacy Notice to check: Royal United Hospitals Bath | Privacy notice	
Is there an option for the data subject to opt out of their information being shared or accessed?	No		
Can data subjects request copies of their information?	If yes, please detail how they would do this?		
	All data will be deliberately de-identified and anonymised therefore can not be re-patriated with its originating subject.		
Name of person(s) completing this DPIA	Howard Jenkinson	Date	04 Mar 2020
Data Protection Officer - Review of DPIA	Graeme Temblett-Willis	Date	09/03/2020

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 due to error on questionnaire – new process and technology 11/03/2020.

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**

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