Royal Free London
NHS Foundation Trust

Data Protection Impact Assessment (DPIA) template

Section A – project details

Project Name	**Patient Reported Outcome Measures (PROMS)**
Organisation	Royal Free London NHS Foundation Trust
Project lead (staff member completing the template)	[redacted]
Job title	Head of Radiotherapy and Treatment Superintendent
Date completed	22.06.18
Phone	[redacted]
E-mail	[redacted]

Introduction - What is a Data Protection Impact Assessment?

Patients have an expectation that their privacy and confidentiality will be respected at all times, during their care and beyond. It is essential therefore, when considering or implementing any new initiatives, that the impact of the collection, use and disclosure of any patient (or staff) information is considered in regards to the individual's privacy. Carrying out a Data Protection Impact Assessment (DPIA) is a systematic way of doing this.

A DPIA is a process that helps an organisation to identify privacy risks and ensure lawful practice when a new project is designed or changes are made to a service. The purpose of the DPIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. It is a particularly useful tool for organisations to identify privacy risks and ensure lawful practice use when:

- Planning a new information sharing initiative such as working with new partners or in different ways;
- Introducing new IT systems for collecting and accessing personal data;
- Intending to use personal data for new uses.

Why is this necessary?

From 25 May 2018 the GDPR introduces a new obligation to do a DPIA before carrying out processing likely to result in high risk to individuals' interests. If your DPIA identifies a high risk which you cannot mitigate, the trust must consult the ICO.

A DPIA helps an organisation to see things from the patient's (or staff members) point of view. It is their data that is being used and their choice about how and why it will be used. "No decision about me, without me" is the vision for the patient-centred NHS. Understanding the impact to the individual(s) personal data enables the system to be designed around their legal rights and expectations of confidentiality.

A DPIA also checks organisational compliance against the legal framework such as the Data Protection Act and General Data Protection Regulation (GDPR), see also risks below.

What are privacy risks?

Privacy risks include the following:

- Risks to individuals or other third parties (for example, misuse or overuse of their personal data, loss of anonymity, intrusion into private life through monitoring activities, lack of transparency).
- Compliance risks e.g. breach of the Data Protection Act (DPA) or GDPR
- Risks to the organisation (for example, failure of the project and associated costs, legal penalties or claims, damage to reputation, loss of trust of patients or the public).

Where do I start? The DPIA process

1. Fill out the **contact details at the top of page 1**. The project lead should be nominated to co-ordinate the DPIA process.

2. Complete the DPIA screening process - see **below section A**. Answering the screening questions will identify whether or not the proposed initiative will impact on patient privacy and whether or not you need to complete a full DPIA. The screening questions are designed to give you a quick sense of the scale of the privacy issues that you may be facing.

3. If you answer “yes” or “unsure” to any of the screening questions in the table, you will need to undertake the DPIA – see **sections B to E on pages 4 to 12**. You may find it helpful to seek assistance from the trust’s Data protection officer / IG team to help you with the process.

4. Once completed send the document to for **review and approval section D**.

Section A - DPIA screening questions

Documenting here which of the screening questions are applicable to your initiative will help to draw out the particular privacy considerations that will help formulate your risk register later in the template. This will also assist in ensuring that the investment the organisation makes is proportionate to the risks involved:
Tip – imagine this initiative involved the use of your own information or that of a relative

		Yes	No	Unsure	Comments
1	Will the initiative use systematic and extensive profiling or automated decision-making to make significant decisions about people?	☐	☒	☐	
2	Is the information about individuals likely to raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?	☒	☐	☐	
3	Will the initiative involve the collection of new information about individuals?	☐	☒	☐	
4	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	☒	☐	☐	

5	Will the initiative require you to contact individuals in ways which they may find intrusive[1]?	☐	☒	☐	
6	Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	☒	☐	☐	
7	Does the initiative involve you using new technology which might be perceived as being privacy intrusive e.g. biometrics or facial recognition?	☐	☒	☐	
8	Will the initiative result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	☒	☐	☐	
9	Will the initiative process personal data which could result in a risk of physical harm in the event of a security breach?	☐	☒	☐	

If you answered **No** to all of the above, and you can evidence/justify your answers in the comments box above, you do not need to continue with the Privacy Impact Assessment as it will not apply to the initiative. Should the initiative change to incorporate informational privacy at any point in the future you will need to complete the screening questions again.

Conducting a full DPIA

1.1 What should a DPIA include?

In simple terms the DPIA should:-

- set out the aims or objectives of the initiative
- explain why the DPIA is necessary (the initial screening questions at the beginning of the template will enable this to be quickly identified)
- document the data flows in terms of, what data is being processed, where it is coming from and who it is going to
- identify the risks to individual's privacy in terms of security, and as potential threats to confidentiality, integrity or availability
- clarify the legal basis
- Identify and evaluate the privacy solutions (how can you reduce or remove the risk?)
- Sign off and record the DPIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders, as needed, throughout the process

1.2 Who should be part of the DPIA team needed to complete the template?

[1] Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages

For the PIA to be effective it needs input from people with a range of expertise, skills and authority. Important features for members of the team include:

- An understanding of the project's aims and the organisation's culture;
- Authority to influence the design and development of the project and participate in decisions;
- Expertise in privacy and compliance matters;
- Ability to assess and communicate organisational risks;
- Ability to assess which privacy solutions are feasible for the relevant project; and
- Ability to communicate effectively with stakeholders and management.

1.3 Does my project need a DPIA?

From 25 May 2018 the GDPR introduces a new obligation to do a DPIA before carrying out processing likely to result in high risk to individuals' interests. A DPIA is suitable for:

- A new IT system for storing and accessing personal data
- A data sharing initiative where two or more organisations seek to pool or link sets of personal data
- A proposal to identify people in a particular group or demographic and initiate a course of action
- Using existing data for a new and unexpected or more intrusive purpose
- A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system
- A new database which consolidates information held by separate parts of an organisation
- Legislation, policy or strategies which will impact on privacy through the collection of personal information, or through surveillance or other monitoring
- Long standing databases where the privacy impact may not have been considered previously or the legal or organisational framework has changed and may give rise to new privacy risks or issues

Section B - Full DPIA template

Background Information

Project/Change Outline - What is it that is being planned? If you have already produced this as part of the project's Project Initiation Document or Business Case etc. you may make reference to this, however a brief description of the project/process being assessed is still required.
Participate in a PROM's project to assist in the development of a commercially available artificial intelligence (AI) driven system. Such a system can facilitate the tailoring of care to the needs of the patient and improve the utilisation of the clinician's time. The data gathered will be reviewed by clinical staff and the information will be used to inform individual patient care. For the radiotherapy services, engagement with this project does not indicate a desire to pursue this product in the future, however it gives the opportunity to develop our understanding of the collection and analysis of PROMs and to help understand how we might develop this process in the future, whether it be with the system being developed or an alternative solution. Approx. 50-75% of annual case load (c.500-600/annum) could be surveyed; this figure is based

on radiotherapy patient surveys however the number could be higher as patients would be actively encouraged to participate and would be supported by the clinical team to do so.

- The system is a stand-alone web based application; the platform is hosted in a N3 data centre. No interface is required with existing oncology management systems or hospital PAS.
- Patient demographics or even pulled from the NHS Summary Care Record
- Patients would be asked to enter PROM's via a tablet device; however they could also complete paper survey and results transcribed by a member of the clinical team
- The data can be used to produce patient or patient cohort specific reports.
- The project will explore the feasibility of developing a patient portal so that patients could submit PROMs from a mobile device or computer from their own home.
- At the end of the project, should the trust end its relationship with Cievert, the patient data is owned by the trust and is not retained by CievertReports will be downloaded from the web app using Trust information asset and output saved directly onto Trust server

Purpose / Objectives - Why is it being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the project.

PROMs are directly reported by the patient, meaning there is no interpretation by a third party. In addition, collecting PROMs only requires the patient and are not restricted by the cost or availability of a clinician and so can be collected more regularly.

What is the purpose of collecting the information within the system? For example patient treatment, patient administration, research, audit, reporting, staff administration etc.

By using technology PROMs can be collected from radiotherapy patients on a daily basis quickly and easily, providing a rich and standardised dataset. This will inform better practice and also facilitate further research. For example – combining PROMs data with clinical interventions and patient outcomes will provide insight into how to better manage side effects and/or minimise them. It might be possible to even prevent some occurring in the first place!

Cievert’s ultimate aim is to assist in the development of an AI PROMS system for radiotherapy/oncology patients. This however is way beyond the scope of this year long project.

What are the potential privacy impacts of this proposal - how will this change impact upon the data subject? Provide a brief summary of what you feel these could be, it could be that specific information is being held that hasn't previously or that the level of information about an individual is increasing.

Data not held on Trust servers. Hosted in N3 data centre, managed by Cievert.

Provide details of any previous Privacy Impact Assessment or other form of personal data compliance assessment done on this initiative.   If this is a change to an existing system, a PIA may have been undertaken during the project implementation

No

Stakeholders - who is involved in this project/change? Please list stakeholders, including internal, external, organisations (public/private/third) and groups that may be affected by this system/change.

Cievert
All radiotherapy staff
Patients and carers

Section C - The data involved

What data is being collected, shared or used? (If there is a chart or diagram to explain attach it as an appendix)

Data Type			**Justifications –** there must be justification for collecting the particular items and these must be specified here – consider which data items you could remove, without compromising the needs of the project?
Information that identifies the individual and their personal characteristics	Name	☒	
	Address	☐	
	Postcode	☐	
	Dob	☒	
	Age	☐	
	Sex	☐	
	Gender	☐	
	Racial/ethnic origin	☐	
	Tel no.	☐	
	Physical description	☐	
	NHS no.	☒	
	Mobile/home phone no.	☐	
	Email address	☐	

	Yes	N/A	Justification
Information relating to the individual's physical or mental health or condition	☒	☐	Relevant to clinical assessment of patient
Information relating to the individual's sexual life	☒	☐	Relevant to patients long term side effects and Quality of life (QOL)
Information relating to the family of the individual and the individuals lifestyle and social circumstances	☐	☒	
Information relating to any offences committed or alleged to be committed by the individual	☐	☒	
Information relating to criminal proceedings, outcomes and sentences regarding the individual	☐	☒	
Information which relates to the education and any professional training of the individual	☐	☒	
Employment and career history	☐	☒	
Information relating to the financial affairs of the individual	☐	☒	
Information relating to the individual's religion or other beliefs	☐	☒	
Information relating to the individual's membership of a trade union	☐	☒	

Section D – Assessment questions

	Question	Response	Required Action
Legal compliance – is it fair and lawful?	1. What is the legal basis for processing the information? *This should include which conditions for processing under the Data Protection Act and GDPR apply and the common law duty of confidentiality.*	Consent	
	2. a - Is the processing of individual's information likely to interfere with the 'right to privacy' under Article 8 of the Human Rights Act? b - Have you identified the social need and aims of the initiative and are the planned actions a proportionate response to the social need?	No Collection of PROMS is aimed at improving the care provided to the patient and to help improve the care for others by using outcomes to develop the service. The planned actions are a proportionate response to the social need.	
	3. It is important that individuals affected by the initiative are informed as to what is happening with their information. Is this covered by fair processing information already provided to individuals or is a new or revised communication needed?	No however a patient information leaflet will be provided which will give patient assurance of how their data will be processed.	Information sheet to be produced by RFH/Cievert
	4. If you are relying on consent to process personal data, how will consent be obtained and recorded, what information will be provided to support the consent process and what will you do if permission is withheld or given but later withdrawn?	Consent will be sought when they attend for initial RT appointment, if they withdraw consent, personal data will be held and used in line with other data held for that patient.	Consent form to be produced by RFH/Cievert
Purp ose	5. Does the project involve the use of existing personal data for new purposes?	No	

	6. Are potential new purposes likely to be identified as the scope of the project expands?	Possibly – the scope of the project could expand; however at this stage it is fairly focused with an established timeline.	
Adequacy	7. Is the information you are using likely to be of good enough quality for the purposes it is used for?	yes	
Accurate and up to date	8. Are you able to amend information when necessary to ensure it is up to date?	Yes – the platform is web based and will be hosted and supported by Cievert.	
	9. How are you ensuring that personal data obtained from individuals or other organisations is accurate?	Data collected is PROMS so data is provided by the patients themselves. Demographics will be checked by clinical staff and the patient will need to complete an ID check to enter their own data into the system.	
Retention	10. What are the retention periods for the personal information and how will this be implemented?	Project duration is for 1 year. After this data collected will be owned by RFH.	
	11. Are there any exceptional circumstances for retaining certain data for longer than the normal period?	No	
	12. How will information be fully anonymised or destroyed after it is no longer necessary?	Tablet devices will be returned to Cievert who are providing them for the duration of the project. Data will be owned by RFH at the end of the project.	
Rights of the individual	13. How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held?	Subject access requests will be processed as per the Trust policy.	

Appropriate technical and organisational measures	14. What procedures are in place to ensure that all staff with access to the information have adequate information governance training?	All radiotherapy staff compliant with mandatory training in information governance.	Check that all staff compliant
	15. If you are using an electronic system to process the information, what security measures are in place?	Tablet devices used to access the system using a secure Wi-Fi connection.	
	16. How will the information be provided, collated and used?	Information provided by patient, reviewed by clinical staff and used to inform patient care.	
	17. What security measures will be used to transfer the identifiable information?	Web-based platform hosted in an N3 data centre. All trust information security measures comply with NHS Digital requirements.	
Transfers both internal and external including outside of the EEA	18. Will individual's personal information be disclosed internally/externally in identifiable form and if so to who, how and why?	Internally only to clinical staff to inform patient care.	
	19. Will personal data be transferred to a country outside of the European Economic Area? If yes, what arrangements will be in place to safeguard the personal data?	No	
Consultation	20. Who should you consult to identify the privacy risks and how will you do this? Identify both internal and external stakeholders. *Link back to stakeholders on page 3.*	DPO	
	21. Following the consultation – what privacy risks have been raised? E.g. Legal basis for collecting and using the information, security of the information in transit etc.	Subject consent to providing data for collection and analysis	
Guidance used	22. List any national guidance applicable to the initiative that is referred to.	NA	

Section E – Privacy issues identified and risk analysis

1) Identify the privacy and related risks (see Appendix 1 for further information)

Nb. By allocating a reference number to each identified privacy issue will ensure you link back to this throughout the rest of the assessment. Column (a), (b) and/or (c) must be completed for each privacy issue identified in column

Table 1

Ref No.	**Privacy issue –** element of the initiative that gives rise to the risk	(a) **Risk to individuals** *(complete if appropriate to issue or put not applicable)*	(b) **Compliance risk** *(complete if appropriate to issue or put not applicable)*	(c) **Associated organisation/corporate risk** *(complete if appropriate to issue or put not applicable)*
1	*Subject consent to providing data for collection and analysis*	*Not fully informed of project aims and how data may be used*	*IG, Data protection*	*Reputation, patient experience*

2) Identify the privacy solutions

Table 2

Ref No.	Risk – taken from column (a), (b) and/or (c) in table 1.	Risk score – see tables at Appendix 2			Proposed solution(s) /mitigating action(s)	**Result:** is the risk accepted, eliminated, or reduced?	Risk to individuals is now OK? Signed off by?
		Likelihood	Impact	RAG status			
1	*Subjects not fully informed of project aims and how data may be used*	2	2	A/ G	*Subjects to be consented to providing data for collection and analysis.* *Subjects to be provided with info leaflet and evidence consent obtained.* *Subjects will be made fully aware of the process and aware of their right to withdraw from the process.*	*Reduced*	

3) Integrate the PIA outcomes back into the project plan

NB. This must include any actions identified in Table 1 and Table 2.

Who is responsible for integrating the PIA outcomes back in to the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?							
Ref No.	**Action to be taken**	**Date for completion of actions**	**Anticipated risk score following mitigation**			**Responsibility for action – *job title not names***	**Current status/progress**
			Likelihood	**Impact**	**RAG status**		
1	*Provide information leaflet and consent obtained*	*Start of software testing period*	*1*	*2*	*G*	*Head of Radiotherapy*	*Ongoing*

Section F - Data Protection Impact Assessment – review and sign off

If you identify a high risk and you cannot mitigate that risk, the trust must consult the ICO before starting the processing*. Please add details below.

* only required post 25 May 2018 implementation of GDPR

RFL Data Protection Officer (name)	[redacted]
Signature	[redacted]
Date of DPIA sign off	19/07/2018
Date of DPIA review	

<u>Copy to be retained by project manager and also IG team.</u>

Appendix 1: Types of privacy risk

Risks to individuals

- Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
- The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people's knowledge.
- New surveillance methods may be an unjustified intrusion on their privacy.
- Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
- The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
- Identifiers might be collected and linked which prevent people from using a service anonymously.
- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
- Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
- If a retention period is not established information might be used for longer than necessary.

Compliance risk

- Non-compliance with the common law duty of confidentiality
- Non-compliance with the duties in the Health & Social Care (Safety & Quality) Act 2015
- Non-compliance with the DPA.
- Non-compliance with the Privacy and Electronic Communications Regulations (PECR).
- Non-compliance with sector specific legislation or standards.
- Non-compliance with human rights legislation.

Associated organisation/corporate risk

- Non-compliance with the DPA or other legislation can lead to sanctions, fines and reputational damage.
- Problems which are only identified after the project has launched are more likely to require expensive fixes.
- The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
- Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, is less useful to the business.
- Public distrust about how information is used can damage an organisation's reputation and lead to loss of business.
- Data losses which damage individuals could lead to claims for compensation.

Appendix 2: Guidance for completing a risk register

- What is the actual risk? Make sure the risk is clear and concise and articulated with appropriate use of language, suitable for the public domain.
- Be careful and sensitive about the wording of the risk as risk registers are subject to the Freedom of Information (FOI) requests
- Don't reference blame to other organisations in the risk register (the register may be made available in the public domain)
- Does the risk belong to a business area within your organisation or another body?

It is common to use a RAG matrix rating system for assessing risk. RAG stands for red, amber, green. To achieve a RAG rating, each risk first needs a likelihood and impact score. Each risk will be RAG rated by taking the likelihood and impact scores, and using the matrix below:

Likelihood

	Score				
Likelihood score	1	2	3	4	5
Descriptor	Rare	Unlikely	Possible	Likely	Almost Certain
Frequency - how often might it happen?	This probably will never happen/recur	Do not expect it to happen/recur, but it is possible it may do so	Might happen or recur occasionally	Will probably happen/recur, but is not a persisting issue or circumstance	Almost certain to happen/recur; possibly frequently

Impact

	Score				
Impact score	1	2	3	4	5
Descriptor	Very low	Low	Medium	High	Very high
Impact should it happen?	Unlikely to have any impact	May have an impact	Likely to have an impact	Highly probable it will have a significant impact	Will have a major impact

Using the risk "RAG" rating system for scoring risks means risks can be ranked so that the most severe are addressed first. Decisions can then be made as to what mitigating action can be taken to alleviate the risk.

Impact	Very High -5	A	A/R	R	R	R
	High - 4	A	A	A/R	R	R
	Medium - 3	A/G	A	A	A/R	A/R
	Low - 2	G	A/G	A/G	A	A
	Very Low - 1	G	G	G	G	G
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
		Likelihood				

Royal Free London NHS Foundation Trust. Template based on the Information Governance Alliance privacy impact assessment guidance and template dated February 2015.