Health Research - Data Protection Impact Assessment Template

Relevant Information

Title	Data Protection Impact Assessment Template
Author	ROYAL COLLEGE OF SURGEONS IN IRELAND – RESEARCH ETHICS COMMITTEE
Publication Date	
Superseded Documents	n/a
Related Documents	Data Protection Policy Data Processing Agreement
Version	1.3
Data Protection Officer	DONALL KING Phone: E-Mail:

This policy may be updated at any time (without notice) to ensure changes to RCSI organisation structure and/or business practices are properly reflected in the policy. Please ensure that you check for the most up to date version of this policy.

Table of Contents

1 Introduction

This Data Protection Impact Assessment (hereafter, "DPIA"), describes how Royal College of Surgeons in Ireland (hereafter, "RCSI") employs the use of additional administrative measures to safeguard and protect personal information relating to patients, research participants and staff. The protection of personal information is something RCSI takes very seriously***. RCSI undertakes to respect the privacy rights of its staff, patients and research participants and will take all necessary steps and measures to protect the fundamental privacy rights and freedoms of individuals.***

At RCSI patients, research participants, staff and other individuals who fall under the category of data subjects, have an expectation that their privacy and confidentiality will be respected at all times, during service provision, patient care and research. It is essential consequently that when RCSI is contemplating or implementing any new initiatives which involves the use of technology, the perceived impact of collection, use and disclosure of any personal data is considered integral to an individual's privacy. Carrying out a Data Protection Impact Assessment (DPIA) is a disciplined way of achieving this objective.

2 Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process that helps RCSI identify risks to the privacy of data subjects and ensure legitimate best practice are followed when a new project is planned, or when changes are made to an already existing product or service. The purpose DPIA serves is to ensure that privacy related risks that arise during data collection, use and disclosure are mitigated using appropriate plans and measures, while allowing the objectives, outputs or deliverables of a project which involves the use of personal data, to be met.

3 What are Privacy Risks?

A privacy risk can be defined as the probability that the fundamental rights and freedom of a data subject may be put at risk through the data processing activities of RCSI. Recital 4 of the General Data Protection Regulation defines the fundamental rights of a data subject as;

- respect for private and family life,
- respect for home and communications,
- protection of personal data,
- freedom of thought, conscience and religion,
- freedom of expression and information…."

Privacy related risks can include one or all of the following:

- Risks to patients, research participants, staff or other third parties (for example, ill-use or overuse of research participant data, loss of anonymity, intrusion into the private lives through monitoring activities, lack of transparency, fairness and lawfulness of data processing activities etc.).
- Compliance risks e.g. breach of the General Data Protection Regulation (GDPR) or other health related legislation
- inherent or residual risks to RCSI (for example, project failure and associated costs, legal penalties or claims, damage to RCSI's reputation, loss of trust of patients or the public).

3.1 Patient / Research Participant /Staff / Service User Perspective

DPIAs helps RSCI see things from the data subject's perspective. How patient data is used and why it will be used should be clearly outlined and articulated to research participants and where appropriate, requires that consent is sought, given, maintained and sustained. Where relevant, RCSI, will adopt a "No decision about me, without me" approach as part of its accountability obligations. Understanding the potential impact of personal data processing on individuals can enable systems to be designed around data subject's legal rights and expectations of confidentiality as outlined under the new regulation. This phenomenon is known as data protection by design and default.

A DPIA also checks organisational compliance against legal framework (where relevant).

Detailing appropriate screening questions that are relevant to RCSI project initiatives will highlight specific and individual privacy considerations that will determine and inform the types of inputs into the Hospital's corporate risk register. This will also assist in ensuring that proposed investment is proportionate to the risks involved:

		Yes	No	Unsure	Comments
1	Will information about individuals raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private?	☐	☐	☐	
2	Will project initiative involve collection of new information about patients, visitors or staff?	☐	☐	☐	
3	Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	☐	☐	☐	
4	Will project initiative require use of patient data in ways which they may find intrusive[1]?	☐	☐	☐	
5	Will patient data be disclosed to other organisations or people who have not previously had routine access to such?	☐	☐	☐	
6	Will project initiative involve using new technology which might be perceived as being privacy	☐	☐	☐	

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

	intrusive or biased e.g. biometrics or facial recognition?				
7	Will project initiative result in the Hospital making decisions or taking actions against individuals in ways which can have a significant negative impact on them?	☐	☐	☐	

4 DPIA Initiation – Health Research

A lead person should be nominated to coordinate and lead the DPIA process. A DPIA starts with a screening process. The screening questions are provided in the table on the previous page. Answering the screening questions will identify whether or not the proposed initiative will impact on the fundamental rights and freedoms of individuals, which in turn determines whether a DPIA is required or not. The screening questions should be designed in such a way that pointers on the degree, scope and scale of privacy issues being experienced, are provided.

Where response to each screening question below is either affirmative or unsure, a DPIA may be required.

4.1 Data Protection Impact Assessment Screening Questions

Where response(s) to the above questions is or are negative, a DPIA may not be required. Should the project initiative change to incorporate informational privacy at any point in the future, the DPIA screening questionnaire would need to be completed again.

4.2 Conducting a Data Protection Impact Assessment (DPIA)

What should a DPIA include?

In simple terms a DPIA should:-

a) articulate in clear terms aims or objectives of project initiative
b) explain why DPIA is necessary
c) document data flows in light of, what data is being processed, source and destination (data inflows and outflows)
d) identify the risks to individual's privacy in terms of personal data security and access, giving consideration to potential threats to personal data confidentiality, integrity or availability
e) clarify the legal basis for processing including retention threshold where appropriate
f) Identify and evaluate likely or available solutions (how can you reduce or remove the risk? Use the Mitigate, Accept, Avoid, Exploit, Transfer, Share risk response types to achieve this objective)
g) Sign off and record the DPIA outcomes
h) Integrate the outcomes into the project plan
i) Consult with internal and external stakeholders (including the ODPC where required. This is particularly relevant where processing would result in a high risk regardless of measures taken by DC/DP to mitigate the risk), as needed, throughout the process
j) Consideration should be given to incorporating a minimum of 8 – 14 week lead time as it can take even longer for the ODPC to feedback to RCSI. This is among other things, is determined by complexity of the intended processing.

4.3 DPIA Team needed to Complete Template

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

a) An understanding of the project's aims and the organisation's culture;

b) Authority to influence the design and development of the project and participate in decision making;
c) Expertise in data protection and compliance matters;
d) Ability to assess and communicate organisational risks;
e) Ability to assess which privacy solutions are feasible for the relevant project; and
f) Ability to communicate effectively with stakeholders and manage expectations.

The DPIA will include but is not limited to the following stakeholders whose input will be sought;

a) Project Sponsor
b) Project Manager
c) Risk Manager
d) Data Protection Officer
e) Project Team

4.4 Can I use a single DPIA for multiple processing operations?

A single DPIA could be used to assess multiple processing operations that are similar in terms of the risks presented, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing. This might mean where similar technology is used to collect the same sort of data for the same purposes.

Where the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights of the data subjects.

5 Privacy Impact Assessment Template

Section 1: Background Information

Project Name	
Organisation/Department	
Assessment Completed By	
Job Title	
Date completed	
Phone/Mobile	
E-mail	
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 you may make reference to this, however a brief description of the project/process being assessed is still required.	
Purpose / Objectives: Why is DPIA it being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the project.	
What is the purpose of collecting the information within the system? For example patient treatment, patient administration, research, audit, reporting, staff administration etc.	
What are the potential privacy impacts of this proposal?: How will this change impact upon the patient or research participant? 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.	
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.	

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.

Section 2: 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	☐	
	IHI no. (or similar)	☐	
	Mobile/home phone no.	☐	
	Email address	☐	

		Yes	N/A	Justification
i.	Information relating to the individual's physical or mental health or condition. Information relating to genetic information(biological samples such as chromosomal or DNA samples) and biometric information(such as fingerprints or facial recognition)	☐	☐	
ii.	Information relating to the individual's sex life.	☐	☐	
iii.	Information relating to the individual's sexual orientation	☐	☐	
iv.	Information relating to the family of the individual and the individual's lifestyle and social circumstances	☐	☐	
v.	Information relating to any offences committed or alleged to be committed by the individual	☐	☐	
vi.	Information relating to criminal proceedings, outcomes and sentences regarding the individual	☐	☐	
vii.	Information which relates to the education and any professional training of the individual	☐	☐	
viii.	Employment and career history	☐	☐	

ix. Information relating to the financial affairs of the individual	☐	☐	
x. Information relating to the individual's religion or other beliefs	☐	☐	
xi. Information relating to the individual's membership of a trade union.	☐	☐	
Will the information be 1) Anonymised	☐	☐	
2) Pseudonymised	☐	☐	
3) Identifiable	☐	☐	
Select the appropriate choice. Please note that where possible information should be anonymised			

Section 3: Assessment

	Question	Response	Required Action E.g. Seek Information Governance advice
Legal compliance – is it fair and lawful?	1. What is the legal basis for processing the information? This is your valid legal reason for processing. These reasons are laid out in Article 6 & 9 of GDPR. Any processing of special categories of data such as health, genetic and biometric information will require TWO legal basis for processing- one from Article 6 and one from Article 9.		
	2. Is the processing necessary and proportionate if the legal basis is Article 6(1)(f) "legitimate interests"? If the answer is "no" processing should not proceed.		
	3. 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 response actions proportionate in response to social need?		
	4. It is important that patients 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?		
	5. 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?		
Purpose	6. Does the project involve the use of existing personal data for new purposes?		
	7. Are potential new purposes likely to be identified as the scope of the project expands?		
Adequacy	8. Is the information you are using likely to be of good enough quality for the purposes it is used for?		
Accurate and up to date	9. Are you able to amend information when necessary to ensure currency and accuracy?		
	10. How are you ensuring that personal data obtained from individuals or other organisations is accurate?		
Retention	11. What are the retention periods for the personal data and how will this be implemented?		
	12. Are there any exceptional circumstances for retaining certain personal data for longer than is necessary?		
	13. How will personal data be fully anonymised or destroyed after it is no longer necessary or fit for purpose?		
Rights of the individual	14. How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held? Will the information be provided to the data subject on their right to rectification, erasure, portability etc? .		
Appropriate	15. What procedures are in place to ensure that all staff with access to the patient data have		

	received adequate information governance training?		
	16. If using an electronic system to process subject access requests, what security measures are in place?		
	17. How will the information be provided, collated and used?		
	18. What security measures will be used to transfer the identifiable information? i. Have you identified any potential risk? ii. The potential impact of any such risk on the data subject. iii. The likelihood and severity of any risk. iv. How you intend to deal with it.		
Transfers both internal and external including outside	19. Will individual's personal information be disclosed internally/externally in identifiable form and if so to whom, how and why?		
	20. 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?		
Consultation	21. Who should be consulted to identify privacy related risks and how will this be achieved? Identify both internal and external stakeholders. *Link back to stakeholders on page 3.*		
	22. 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. You should also include consultation with the data subject – have their views been sought?		

Guidance used	23. List any national guidance applicable to the initiative that is referred to.		

5.1 Section 3 – Privacy issues identified and risk analysis

5.1.1 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)
PR1	*Individuals are not aware of the initiative as no communication materials have been planned*	*Individuals not aware that their data is being processed*	*Non-compliance with Article 5(1) principle /Concept 1 – fairness, lawfulness and transparency*	*1. May lead to public mistrust* *2. May lead to sanction by the (ODPC)*

5.1.2 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			
PR1	*Individuals not aware that their data is being processed* *Non-compliance with DPA principle 1 – fair and lawful processing* *1. May lead to public mistrust* *2. May lead to sanction by the ODPC*	5	5		*Communication plan to be developed to ensure compliance with fair and lawful processing* *Assurance that there will be an active communication campaign* *All relevant staff informed of need to understand and disseminate communication material.*	*Reduced to an acceptable level (it is not possible to eliminate at this stage as the Comms plan will need to ensure it addresses all aspects to enable individuals to be fully informed.*	*Yes* *Sign-off tbc*

5.1.3 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**		
PR1	*Communications plan to be developed*		*2*	*2*		*Project Manager to liaise with Communication lead and embed into project plan*	*Meeting arranged with Communication Lead*

6 Appendix 1: Types of privacy risk

6.1 Risks to individuals

i. Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
ii. 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.
iii. New surveillance methods may be an unjustified intrusion on their privacy.
iv. Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
v. The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
vi. Identifiers might be collected and linked which prevent people from using a service anonymously.
vii. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
viii. Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
ix. Information which is collected and stored unnecessarily, or is not properly managed so that duplicate records are created, presents a greater security risk.
x. If a retention period is not established information might be used for longer than necessary.

6.2 Examples of Compliance Risk

i. Non-compliance with the common law duty of confidentiality
ii. Non-compliance with the Data Protection Acts 2018/ General Data Protection Regulation (GDPR).
iii. Non-compliance with the Privacy and Electronic Communications Regulations (PECR)/e-Privacy Regulation.
iv. Non-compliance with sector specific legislation or standards e.g. Health Information and Quality Authority (HIQA), Health and Safety Authority (HSA).

v. Non-compliance with human rights legislation United Nations Declaration on human Rights (UNDHR).

6.3 Associated organisation/corporate risk

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

7 Appendix 2: Guidance for completing a risk register

- What is the actual risk? Make sure the risk is clear and concise, well understood 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. This is relevant is your organization is subject to the FOI Act.
- Don't reference blame to other organisations in the risk register
- 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				