Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Hospital Logo

Data Protection Impact Assessment (DPIA)

Template – Research

Please review the TCD *Data Protection Risk Assessment* document before undertaking a DPIA.

It is important to note that a DPIA is required as standard for research studies conducted at St. James's Hospital, Tallaght University Hospital and all clinical sites in which Trinity researchers are active.

Study Name:	**Date:**
Owner:	**Site:**
Email:	**Phone Number:**

Template Version Control

Reference	Date	Author	Comments
2.0	May 2019	TCD DPO	

DPIA Circulation

Name	Date	Reviewed/Consulted
PI Details	[Insert Date]	*Reviewed/Consulted*
Co-I/Other Details	[Insert Date]	*Reviewed/Consulted*
DPO Details	[Insert Date]	*Reviewed/Consulted*

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

Contents

DPIA - Objective

The purpose of a DPIA is to assess and demonstrate compliance with data protection legislation. The DPIA also provides evidence that the risks to individuals have been considered and sufficient measures have been taken to protect those individuals. The DPIA should assess the activity to be carried out against all the principles of data protection and determine whether the processing of personal data is both necessary and proportionate or whether changes to the process or additional controls are required.

Data Protection Checklist for Health Research

If your project relates to health research, then you must comply with the requirements of the Health Research Regulations 2018.

You ***must*** carry out the following:

Obtain ethical approval for the health research by a research ethics committee.	
Identify and document the data controller, joint controllers and data processors.	
Ensure relevant contractual arrangements are in place.	
Identify and document funding bodies.	
Identify third parties with whom data will be shared even if pseudonymised.	
Ensure all members of the research team have completed data protection training.	
Carry out a risk assessment of the data protection implications of the research.	
Carry out a DPIA if the research represents a high risk to individuals or involves the use of genetic data, monitoring of behaviours, large scale processing of sensitive personal data, use of the data for new purposes or the linking of datasets.	
Ensure you only use the minimum data necessary to carry out the research.	
Implement controls to ensure the integrity and accuracy of data and determine when the data has been altered, disclosed or erased and by whom.	
Implement security measures to protect the personal data; e.g. device encryption.	
Ensure the data is archived, anonymised or destroyed when the research is completed.	
Ensure that participants are provided with sufficient information about the use of their personal data via Participant Information Leaflets, Consent Forms and the project website.	
Obtain explicit consent for the processing of personal data for the health research Including the screening of individuals for research purposes.	

DPIA - Instructions

You should complete all of the questions in this template and forward the completed document to the relevant data protection officer to receive feedback on any risks identified and recommendations on the actions or controls needed to address those risks.

Trinity College: dataprotection@tcd.ie

St James's Hospital: research@stjames.ie

Tallaght University Hospital: dpo@tuh.ie

It is the responsibility of the Project Supervisor to ensure the required controls are put in place and to sign off on any risks arising from the processing.

The DPIA should be updated to reflect any material changes to the processing as the project or activity progresses.

Study Details

Nature of Process/ System/ Project

Describe in detail the nature of the process, system or project to be assessed.

Include:

- The **name** of the project.
- The **scope** of the processing.
- The **purpose** for the activity.
- The **frequency** of the processing.
- The **number of individuals** involved and/or affected.
- Details of the **parties and third parties** involved including other data controllers or processors.
- Details of any **systems** to be used.

Nature of Process/ System/ Project
[INSERT DETAILS HERE – MAXIMUM 300 WORDS]

Further details in respect of the intended processing

Does the activity involve processing data on a large scale? If so, provide detail.	
Does the activity involve matching or combining datasets? If so, provide detail.	
Does the activity involve data concerning vulnerable individuals or children? If so, provide detail.	
Does the activity involve new, or innovative uses of, technological or organisational solutions? If so, provide detail.	
Could the activity prevent individuals from exercising a right, using a service, or fulfilling a contract? If so, provide detail.	
Why the use of personal data is necessary for this activity?	
Who will benefit from the activity?	
Could the use of the personal data for this activity result in any harm to the individual?	

Any other information in respect of the study which may be relevant

Additional information
[INSERT DETAILS HERE – MAXIMUM 300 WORDS]

Personal Data

List the types of personal data that will be **collected, used, accessed or shared** for the purpose of this activity.

Data Collected	Justification	Processing Activity
EXAMPLE: Participant names	*Identification, so that we can apply matching codes across longitudinal data sets.*	*Excel database, situated in 'X' Drive on 'X' desktop computer at 'X' site.*
EXAMPLE: Written consent	*Legal basis for processing.*	*Paper forms, stored in locked filing cabinet at 'X' site. Access restricted to [detail] only.*

Transparency of Processing

How will you notify participants about the data processing that will be carried out using their personal data? Provide details and **attach copies** of the Consent Form(s) and Participant Information Leaflet(s).

Transparency of processing
[INSERT DETAILS HERE]

Data Security – Storage and Sharing

Describe in detail the technical and organisational security measures which will be taken to protect personal data including but not limited to; access controls, data sharing restrictions, encryption, pseudonymisation, anonymisation etc.

Data security – storage and sharing
[INSERT DETAILS HERE]

Data Minimisation

Have you ensured that you will only collect the minimum data that you need or that is necessary for the activity? Provide details.

Data minimisation
[INSERT DETAILS HERE]

Lawful Basis – Ordinary Personal Data

If processing 'Ordinary' personal data then you must satisfy at least one of the lawful bases as set out under Article 6 GDPR:

Consent	
Performance of a contract	
Legal obligation	
Public interest or exercise of official authority	
Vital interests of data subjects	
Legitimate interests	

If using *Consent*, then describe the consent process and attach supporting documentation.

Lawful Basis – Special Category Data (Sensitive Personal Data)

Sensitive personal data is defined as:

- Processing of personal data revealing
  - racial origin
  - ethnic origin
  - political opinions
  - religious beliefs
  - philosophical beliefs
  - trade-union membership
- Processing of genetic data for the purpose of uniquely identifying a natural person
- Processing of biometric data for the purpose of uniquely identifying a natural person
- Data concerning health
- Data concerning a natural person's sex life
- Data concerning a natural person's sexual orientation

If processing sensitive personal data then, in addition to the Article 6 lawful basis, you must also satisfy one of the conditions as set out under Article 9 GDPR:

Explicit Consent	
Employment / DSP rights	
Vital Interests of the data subject or another person	
Carried out (internally) by a not-for-profit organisation	
Information that has been already made public by data subject	
Necessary for the establishment, exercise or defence of legal claims	
Necessary for substantial public interest	
Necessary for the provision of medical care/ administration	
Necessary for reasons of public interest in the area of public health	
Archiving purposes in the public interest/ Scientific or Historical Research purposes/ Statistical purposes	

If using *Explicit Consent*, then describe the consent process and attach supporting documentation.

Health Research Regulations - Explicit Consent required for Health Research

In addition to satisfying Articles 6 & 9 GDPR requirements you must also obtain explicit consent for processing personal data for health research purposes. This mandatory requirement is set out under Regulation 3(1)(e) of the 2018 Health Research Regulations.

Describe how you will you ensure that explicit consent is obtained for processing personal data for health research purposes. **Attach supporting documents**, including Consent Forms and Participant Information Leaflets.

If you intend to seek a Public Interest Waiver from the Health Research Consent Declaration Committee (HRCDC) please review the *Pre-submission Checklist* which is available to download from the HRCDC website before proceeding further. If you require further assistance please contact the TCD Data Protection Unit at dataprotection@tcd.ie or St James's DPO at research@stjames.ie.

Heath Research Regulations, Consent, Participant Information Leaflets
[INSERT DETAILS HERE]

High-Risk Processing

Does the research involve any of the following:

- evaluating or predicting outcomes in individuals;
- decision making by automated means e.g. using algorithms;
- monitoring the behaviours of individuals;
- the surveillance of individuals, use of location or the use of biometric technology such as facial recognition.

If so, provide details and describe the impact to the individuals.

High risk processing
[INSERT DETAILS HERE]

Internal Data Sharing

Will the data be shared internally? i.e. with departments or business units within the organisation? If so, provide details on the data sharing including information on the necessity for the processing, the format of the data that is to be shared, with whom the data will be shared and confirmation of the security measures in place to protect the data in transit.

Internal data sharing
[INSERT DETAILS HERE]

Third Parties

Will the data be shared with third parties including IT service providers, Cloud-based solutions, sub-contractors etc.? If so, provide details including information on the contractual arrangements in place and confirm what due diligence has been carried out.

Third parties
[INSERT DETAILS HERE]

International Data Transfers

Will the data be transferred or stored outside the EEA at any point or placed with Cloud providers that store data outside the EEA? Provide details. If you are transferring personal data outside the EEA have you ensured that suitable conditions for transferring the data are in place? Provide details or state if unsure. These include:

- Adequate jurisdiction
- US Privacy Shield
- Standard Contract Clauses
- Binding Corporate Rules
- Authorisation from the Data Protection Commission

International data transfers
[INSERT DETAILS HERE]

Data Retention

How long will the data be retained for and why? Provide details.

Data retention
[INSERT DETAILS HERE]

Data Subject Rights

What plans are in place for responding to a request from an individual in relation to their data protection rights?

These include:

- right of access;
- right to rectification;
- right to erasure;
- right to object to processing based on legitimate or public interest;
- right to data portability;
- right to object to profiling or making decisions about individuals by automated means.

Data subjects rights
[INSERT DETAILS HERE]

Training

What guidance and training will be provided to individuals involved in this project or activity to enable them to understand their data protection responsibilities? Provide details.

Training
[INSERT DETAILS HERE]

Processing Risks - Examples

See Table below. Describe the source of risk and nature of potential impact on individuals. Include associated Compliance and Corporate risks as necessary.

Examples of privacy risks that might be applicable:

Risks to individuals

- Hacking of computers where project data is stored.
- 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 risks

- Non-compliance with the common law duty of confidentiality
- Non-compliance with the Data Protection Acts 2018/ General Data Protection Regulation (GDPR), Privacy and Electronic Communications Regulations (PECR)/ e-Privacy Regulation.

Associated organisation/corporate risks

- Non-compliance with the data protection 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.
- 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.

Different projects carry different risks and these should be considered. The above examples are a guide, not an exhaustive list.

Processing Risks - Table

Describe the source of risk and nature of potential impact on individuals. Include associated Compliance and Corporate risks as necessary.

Risk detail	Risk rating (High, medium, low)	Solutions/Mitigating Actions	Effect	Outcome	Measure approved
Hacking into computers where project data is stored.	*Low*	*All computers storing data are password protected. The external hard drive and remotely accessible computer are also encrypted and locked in an office (on Trinity's campus). Access is restricted to designated staff only.*	*Reduced*	*Low*	*Yes/No*

Risk detail	Risk rating (High, medium, low)	Solutions/Mitigating Actions	Effect	Outcome	Measure approved
Hacking into computers where project data is stored.	*Low*	*All computers storing data are password protected. The external hard drive and remotely accessible computer are also encrypted and locked in an office (on Trinity's campus). Access is restricted to designated staff only.*	*Reduced*	*Low*	*Yes/No*

Disclaimer

This material contained in this guidance contains general information and guidance only. Please note that this guidance does not constitute legal advice and is provided for general purposes only. Neither is it intended to provide a comprehensive or detailed statement of the law.

No liability whatsoever is accepted by Trinity College Dublin, the University of Dublin for any action taken in reliance on the information contained in this guidance. You should not act or refrain from acting, on the basis of any information provided in this guidance but rather you should always seek specific legal or other professional advice. Any and all information is subject to change without notice.