**Data Protection Impact Assessment (DPIA)**

**Health Research**

|  |  |
| --- | --- |
| **Research Study / Project (‘Study’) Title:** | **Date:** |
| **Completed by:** | **Location:** |
| **Email:** | **Phone Number:** |

# DPIA Circulation

|  |  |  |
| --- | --- | --- |
| **Name** | **Date** | **Reviewed/Consulted** |
| **Principle Investigator (PI) Details** | [Insert Date] | Reviewed/Consulted |
| **Co-I/Other Details** | [Insert Date] | Reviewed/Consulted |
| **DPO Details** | [Insert Date] | Reviewed/Consulted |

DPIA - Objective

The purpose of a DPIA is to assess and demonstrate study 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 measure the activity to be carried out against all of the Principles of data protection and determine whether the processing of personal data for the purposes of the study is both necessary and proportionate or whether changes to the process or additional controls are required.

# 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](mailto:dataprotection@tcd.ie)

St James’s Hospital: [research@stjames.ie](mailto:research@stjames.ie)

Tallaght University Hospital: [dpo@tuh.ie](mailto:dpo@tuh.ie)

It is the **responsibility of the PI** 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 study progresses.

**Further information, training, guidance, policies, staff handbook, links and templates is available at** [**www.tcd.ie/dataprotection**](http://www.tcd.ie/dataprotection)**.**

# Data Protection Checklist for Health Research

**If your study relates to health research**, then you must comply with the requirements of the [Health Research Regulations 2018](http://www.irishstatutebook.ie/eli/2018/si/314/made/en/pdf).

You ***must*** carry out the following. Please complete the Y/N boxes below.

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

# 

# Study Details

**Describe the study in detail**

|  |  |
| --- | --- |
| Study title. | Provide detail |
| Number of individuals affected. | Provide detail |
| Description of the study.  (300 words max) | Provide detail |
| Provide details of parties involved (internal stakeholders, collaborators, external organisations (public/private, third parties) etc. (add rows if necessary). Specify the data controller, data processor and joint controller(s). | Provide detail |
| Provide information as to why the use of personal data (data which relates to an individual) is necessary for the study. | Provide detail |

# Further details in respect of the intended use of the data

|  |  |
| --- | --- |
| Attach all relevant data flowcharts, data maps, records of processing activities etc. which clearly explain the internal and external data pathways**.** | Provide detail |
| Does the activity involve matching or combining datasets? If so, provide detail**.** | Provide detail |
| Does the study involve processing data concerning vulnerable individuals or where there may be an imbalance between the data subject and Trinity College (such as employees, patients etc.)? If so, provide detail**.** | Provide detail |
| Does the activity involve data concerning children(anyone under 18)?  If yes, will the child receive information about the risks and benefits of the study?  Will the assent of the child and consent of the parent/guardian be obtained? Outline this process.  Please explain how you will review consent if the research subjects reach 18 years old during the course of the study. | Provide detail |
| Does the activity involve new, or innovative uses of, technological or organisational solutions? If so, provide detail. | Provide detail |
| Could the activity prevent individuals from exercising a right, using a service, or fulfilling a contract? If so, provide detail. | Provide detail |
| Is the use of the personal data being used in whole or part for a different purpose than the original purpose for which it was collected (secondary use). If so provide detail. | Provide detail |
| Insert other relevant details here | |

# Personal Data Processing

What personal data will be **collected, used, accessed, retained or shared** (internal and external of Trinity College) for the purpose of the study. If there is a chart, data map or diagram to explain the data flow attach it as an appendix.

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

Examples:

* Name, address, mobile number, email address, other contact details (please specify)
* D.O.B., age
* Gender
* Photo/ video / recorded interviews which could identify the person
* Data concerning health
* Information concerning:
  + racial origin
  + ethnic origin
  + political opinions
  + religious beliefs
  + philosophical beliefs
  + trade-union membership
  + genetic information
  + biometric data
  + a person's sex life or sexual orientation
* Criminal information
* Location data
* Disability data
* Employment and career history
* Education and professional training
* Questionnaires etc.
* Information relating to the family of the individual and the individual’s lifestyle and social circumstances
* Other data items (please specify)

|  |
| --- |
| [INSERT DETAIL HERE] |

# Necessity & Proportionality

There must be justification for processing personal data. Are all of the data items listed above required or could some be removed without compromising the study goals?

|  |
| --- |
| [INSERT DETAIL HERE] |

# Source of data

How / from where has the data been obtained?

|  |
| --- |
| [INSERT DETAIL HERE] |

# Processing activity

How / where is the data processed? List different systems, devices and formats.

|  |
| --- |
| [INSERT DETAIL HERE] |

# Data category

Is the data:

* Identifiable
* Pseudonymised (coded - a link remains which could potentially identify relevant individuals)
* Anonymised (irreversibly - no link anywhere which could identify relevant individuals)

Further information on Anonymisation and Pseudonymisation is available [here](https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190614%20Anonymisation%20and%20Pseudonymisation.pdf).

|  |
| --- |
| [INSERT DETAIL 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](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1797-1-1).

|  |  |
| --- | --- |
| Consent |  |
| Performance of a contract |  |
| Legal obligation |  |
| Public interest or exercise of official authority **(Recommended for University research)** |  |
| Vital interests of data subjects |  |
| Legitimate interests |  |

# Lawful Basis – Special Category Data (Sensitive Personal Data)

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](https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1797-1-1):

|  |  |
| --- | --- |
| 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 **(Recommended for University research)** |  |

# 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](http://www.irishstatutebook.ie/eli/2018/si/314/made/en/pdf).

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, Privacy Notices, Privacy Policies, Data Protection Statements, text that is to be included on contracts, introductory emails to participants etc.

The approved Trinity College templates must be used to ensure compliance with GDPR and the Data Protection Acts. These can be downloaded at:

<https://www.tcd.ie/dataprotection/trinitycollegetemplates/>

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](https://hrcdc.ie/apply/) before proceeding further. If you require further assistance please contact the TCD Data Protection Office at [dataprotection@tcd.ie](mailto:dataprotection@tcd.ie) or St James’s DPO at [research@stjames.ie](mailto:research@stjames.ie).

* Are you able to amend/correct information when necessary?
* How will you action requests from individuals (or someone acting on their behalf) for access/amendment/restriction to use of their personal information?
* Do you have a procedure in place if an individual wishes to withdraw their consent (if processing on the legal basis of consent)?

|  |
| --- |
| [INSERT DETAIL HERE] |

# Purpose Limitation

Is the processing for the intended purpose only, or is there possibility that additional purposes may be added at a later date? You must ensure that ‘function creep’ is avoided.

|  |
| --- |
| [INSERT DETAIL 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.

|  |
| --- |
| [INSERT DETAIL HERE] |

# Data Quality

How will the data be kept accurate, consistent and up-to-date?

|  |
| --- |
| [INSERT DETAIL 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.

|  |
| --- |
| [INSERT DETAIL HERE] |

# Data Security and Integrity

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

|  |  |
| --- | --- |
| 1. Does the system processing the personal information have access controls? (E.g. role-based, location-based, time-based)   * Indicate how events are logged and how long this log is kept. * If role-based controls, please provide a table outlining roles and responsibilities. * If location based, how is physical access controlled? | Provide detail |
| 2. If the data is transferred from one system to another, how is this accomplished?   * Laptop (portable device); Email; File-share. * Third party services (where is the server located?). * Removable media - USB/removable hard drive? * Printed/paper copies (how is it printed, stored, destroyed and transferred). * Other (describe). | Provide detail |
| 3. If data is on physical devices/paper how is it moved?   * E.g. Post/ Courier/ Employee/Other. | Provide detail |
| 4. Is data encrypted in transit? If yes please provide encryption method   * E.g. 128 bit, 256 bit, Full disk, file level, VPN etc. | Provide detail |
| 5. Is the data encrypted at rest? If yes – please provide level of encryption   * E.g. 128 bit, 256 bit, Full disk File level, VPN etc. | Provide detail |
| 6. Have you familiarised yourself with the Trinity College [Personal Data Breach Procedural Guidelines](https://www.tcd.ie/dataprotection/databreach/)? | Provide detail |
| 7. How are you ensuring that information obtained from other organisations is accurate? | Provide detail |
| Insert other relevant 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

|  |
| --- |
| [INSERT DETAIL 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.

|  |
| --- |
| [INSERT DETAIL HERE] |

# Third Party - Data Sharing

Will the data be shared with third parties? If so, provide details including information on the contractual arrangements in place and confirm what due diligence has been carried out.

This list should include all Data Processing and Data Sharing Agreements, SLAs and MOUs with external parties, Cloud-based Solutions Agreements, Material Transfer Agreements etc.

|  |
| --- |
| [INSERT DETAIL 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 in accordance with [Chapter V GDPR](https://gdpr-info.eu/chapter-5/) requirements for transferring the data are in place? Provide details or state if unsure. These include:

* Adequate jurisdiction
* Standard Contract Clauses
* Binding Corporate Rules
* Authorisation from the Data Protection Commission

|  |
| --- |
| [INSERT DETAIL HERE] |

# Data Retention

|  |  |
| --- | --- |
| 1. How long will the data be retained for and why? | Provide detail |
| 2. How will personal data be fully anonymised or destroyed after it is no longer necessary? | Provide detail |

# Training

The provision of training in data protection law and practice is a mandatory requirement for Trinity College staff. What guidance and training will be provided to the staff and students involved in this study to enable them to understand their data protection responsibilities? Provide details.

|  |
| --- |
| Training |
| Trinity College - Blackboard online GDPR training module. Available at:  <https://www.tcd.ie/itservices/vle/kb/overview-GDPRtraining.php>  Provide detail  Trinity College - CA7000: Research Integrity and Impact in an Open Scholarship Era. Available at:  <https://www.tcd.ie/business/doctoral/programme-structure.php>  Provide detail  Other training carried out (e.g. HSELand) - please provide details. |

# 

# 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 applicable privacy risks:

**Risks to individuals - Examples**

* Hacking of computers where study 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.
* Incorrect or overuse of individuals’ data.
* Lack of transparency, fairness or lawfulness of processing activities.
* Failure to explain effectively how data would be used.
* 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.
* Anonymisation techniques chosen may turn out to be ineffective.
* Use of technology capable of making visual or audio recording may be unacceptably intrusive.
* 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 1988- 2018/ General Data Protection Regulation (GDPR), Privacy and Electronic Communications Regulations (PECR).

**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 study has commenced 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 Trinity College.
* Public distrust about how information is used can damage Trinity’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 as well as implemented or suggested solutions / mitigating actions.

Include associated Compliance and Corporate risks as necessary.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Risk detail | **Risk likelihood**  **(1 – 5)** | **Risk severity**  **(1 – 5)** | **Risk**  **score**  **(1 – 25)** | **Solutions / Mitigating Actions** | **Solutions / Mitigating actions implemented?** | **Residual risk**  **(Unchanged / Reduced / Eliminated)** | **New score** |
| *EXAMPLE*  *Hacking into computers where study data is stored.* | *2* | *4* | *8* | *All computers storing data will be password protected. The external hard drive and remotely accessible computer will be encrypted and locked in an office on Trinity’s campus. Access is restricted to designated staff only.* | *Yes* | *Reduced* | *5* |
| *EXAMPLE*  *If a retention period is not established information might be used for longer than necessary.* | *5* | *4* | *20* | *All relevant data will be saved electronically, held in confidence and stored in secure password-protected computers. All the electronic documents will be deleted and destroyed after a period of [INSERT] months / years in accordance with standard University procedures.* | *No* | *Unchanged* | *20* |
| *EXAMPLE*  *Information which is collected and stored unnecessarily, or is not properly managed, so that duplicate records are created, presents a greater security risk.* | *4* | *5* | *20* | *All digital files (all data collected during the study) in an external hard drive computer. A back-up copy of files will be retained on OneDrive cloud storage platform. A single file (Excel format) linking the codes to data subjects will be encrypted (using 256-bit keys (AES-256) encryption software) and will be held by the project owner.* | *Yes* | *Reduced* | *5* |
| *EXAMPLE*  *Non-compliance with the common law duty of confidentiality.* | *3* | *5* | *15* | *Information and consent forms will explicitly inform participants that their data will be kept confidential, but will emphasise the statutory limitations of confidentiality. Confidentiality may be breached in circumstances in which the research team has a strong belief or evidence exists that there is a serious risk of harm or danger to either the participant or another person. Disclosure may be required as part of a legal process or Garda investigation. In such instances, information may be disclosed to significant others or appropriate third parties without permission being sought from the participant. Where possible, a full explanation will be given to the participant regarding the necessary procedures and also the intended actions that may need to be taken.* | *Yes* | *Eliminated* | *5* |
| *EXAMPLE*  *The context in which information is used or disclosed can change over time, leading to it being used for different purposes without participant’s knowledge.* | *4* | *4* | *16* | *Participant’s data will not be subject to further processing that is incompatible with the purpose of the present study.*  *Privacy notice will make participants aware of how data is processed.* | *No* | *Unchanged* | *16* |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# DPO Feedback: Further risks identified

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Risk detail | **Risk likelihood**  **(1 – 5)** | **Risk severity**  **(1 – 5)** | **Risk**  **Score**  **(1 – 25)** | **Solutions / Mitigating Actions** | **Solutions / Mitigating actions implemented?** | **Residual risk**  **(Unchanged / Reduced / Eliminated)** | **New score** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# Disclaimer

This material contained in this template 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 document. Rather, you should always seek specific legal or other professional advice. Any and all information is subject to change without notice.

# Template Version Control

|  |  |  |
| --- | --- | --- |
| **Reference** | **Date** | **Author** |
| Version 3.0 | April 2022 | Trinity College DPO |