Companion Guidance Document to the

Health Research Data Protection Impact Assessment Form

Version:	1
Date:	January 2024

Definitions, Abbreviations & Acronyms

Abbreviation / Acronym / Term	Complete Term/Definition
CI	Chief Investigator
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
DDPO	Deputy Data Protection Officer
EU/EEA	European Union/European Economic Area
GDPR	General Data Protection Regulation
Healthcare Organisation	The is a public funded organisation, included but not limited to the HSE and Section 38 & 39 Organisation that is prescribed to provide healthcare in the republic of Ireland under, Regulation, legislation Statutory instrument or Ministerial Order.
Health Research DPIA	Data Protection Impact Assessment conducted for the purpose of a Healthcare Research Project or Study
HSE	Health Service Executive
HSE L&DG Office	The Legal and Data Governance Office, Research and Development, HSE
Pharmaceutical Organisation	A pharmaceutical company, Medical devices or drug company, is a commercial business licensed to research, develop, market and/or distribute drugs, most commonly in the context of healthcare.
PI	Principal Investigator

Introduction

The General Data Protection Regulation (GDPR) and the Data Protection Act 2018 provide an EU and National legislative basis to regulate the processing of personal data in Ireland. The Health Research Regulations 2018 to 2021 (made under the 2018 Act) provide a statutory framework governing the processing of personal data for health research in Ireland irrespective of where the data controller carrying out the research is geographically located.

The above legislation complements and supplements long established ethical principles and the constitutionally recognised common law duty of confidentiality that relates to the disclosure of patient/service user information by health service providers, universities, independent researchers and other organisations who may conduct health research. Maintaining privacy and confidentiality of Patient / Service User information is a basic principle all organisations who process this type of information. It is the role of all staff to ensure that privacy and confidentiality of Patient / Service User data is maintained.

Under Article 35 of the GDPR, data controllers need to undertake a Data Protection Impact Assessment (DPIA) for any processing that is 'likely to result in a high risk to individuals', including some specified types of processing.

The Data Protection Commission describe a DPIA as "a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible". DPIAs are, therefore, important tools for negating risk, and for demonstrating compliance with the GDPR.

Further, while the DPIA is designed to allow those contemplating the processing to identify and to reduce or eliminate risk it also importantly serves to provide transparency and re-assurance to the public (especially those whose personal data might be used in a high risk processing project) that a systematic process has been undertaken designed to protect their fundamental rights and freedoms and ensure suitable safeguards in relation to any processing to be undertaken.

Where the project involves the processing of personal data for health research purposes, the Health Research Regulations provide (as a data subject safeguard) that a screening process must always be formally carried out in order to determine whether the level of risk associated with the research project is such as to require a full DPIA.

The DPIA is another part of your organisation corporate governance model, which provides framework of principles, policies, procedures and guidelines by which your organisation directs and controls its functions and manages its business/operations.

Purpose

The purpose of this document is to provide guidance on all aspects of conducting a Data Protection Impact Assessment (DPIA) for the project lead or person responsible for completing the form.

For all new processing activities where personal data is being collected, used and or stored etc., including research studies, it is necessary to carry out an assessment of the associated data protection risks and implications before the processing or research study can commence. Where the assessment indicates a high risk to the rights and freedoms of prospective research participants, a DPIA must be completed.

A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of data subjects involved. DPIAs are important tools for organisations to demonstrate key data protection principles such as accountability, transparency,

purpose limitation, data integrity etc. as they help the Healthcare Organisation to consider, assess and where required document data protection risks and technical and organisational control measures for any new processing activity. The DPIA process also helps the Healthcare Organisation demonstrate that appropriate measures have been taken to ensure compliance with the General Data Protection Regulation (GDPR).

It is necessary for the Data Protection Officer or appropriate local organisation or functional representative (with data protection training) to review the completed DPIA so they can assess the risks and provide review comments and feedback before the DPIA can be finalised and signed off by the project sponsor (and study sponsor for research).

Use of the DPIA and this companion guidance document will ensure that the assessment undertaken for the processing activity is underpinned by a solid, legitimate and valid legal basis to ensure all necessary legal and regulatory requirements are complied with.

Scope

This companion document is to support DPIA assessments across all data processing activities taking place in the Healthcare Organisation, Universities or other private organisations (Pharma, Medical Devices etc.) involved in the processing of personal data for the purpose of Health Research.

Guidance for completing the DPIA Form

Please note if you wish to copy and paste in any section of the web form, you will need to paste in plain text to ensure the format is correct.

Section A DPIA Ownership

This section relates to ownership of the DPIA document and all questions in this section are to be answered before moving to the next section.

Key points to note:

- Project Sponsor refers to the appropriate or responsible senior person/lead from the Organisation (legal entity) involved. For example, this may be the Clinical Lead for a research project, a Director/Assistant Director, Programme Director etc.

Section 1 Description of the Data Processing Activity

1.1 Parties to the Processing

This section relates to the Parties or Organisations involved in the processing activity. Please include the details of any agreements in place between the Healthcare Organisation and other third parties involved.

The Healthcare Organisation is typically the data controller for the processing activity it undertakes. More than one of the Healthcare Organisation departments may be involved with the processing activity, however this does not make each department independent data controllers. Additionally, the Healthcare Organisation department would not be a data processor as defined under Article 4(8) of the GDPR.

Data processors typically work under the instruction of the data controller/ Healthcare Organisation, e.g. Microsoft, who provide the technical infrastructure for Healthcare Organisation to communicate by email, Teams etc. There are some instances however where the HSE acts as a data processor (e.g. payroll, laboratory services, reporting etc.).

For the question *"Is the personal data going to be shared with anyone other than the listed data controllers/processors?"* you should consider external parties such as other Universities, Hospitals or Big Pharma Organisations who are not part / listed on the initial research activity.

Key definitions for this Section:

- **Data controller:** 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data […], GDPR Article 4(7).

- **Joint controller:** If two or more controllers jointly determine the purposes and means of processing the same personal data, they are **joint controllers**. However, they are not joint controllers if they are processing the same data for different purposes.

- **Data Processor:** 'processor' means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller, GDPR Article 4(8).

- **Sub-processor**: A third-party data processor engaged by a data processor who has or will have access to or process personal data from the data controller.

Example of a Data Controller

- The Healthcare Organisation Hospital sends a patient's blood to a Third Party Laboratory for analysis. The laboratory tests the blood and provides report with the test results to the Healthcare Organisation Hospital. The Healthcare Organisation uses the report results to determine the appropriate treatment for the patient.

- The Healthcare Organisation Hospital will be the controller for the personal data processed in connection with the blood test report results and further treatment for the patient because they are determining the purposes and means of the processing of that personal data.

Example of a Data Processor

- The Healthcare Organisation Hospital engages a survey provider to send surveys to patients who previously confirmed their interest in taking part in a Healthcare Organisation survey. The Healthcare Organisation provides the patient's contact details to the survey provider, which the survey provider uses to email/text the survey invitation.

- The Healthcare Organisation would be the data controller of the personal data processed in connection with the survey. The Healthcare Organisation determines the purposes for which the personal data is being processed (to send individually addressed surveys) and the means of the processing (sharing the data subjects' mobile number / email address with the survey provider). The survey provider is a data processor using their system to text/email the participants the survey invitation and collecting their data as part of the survey. They share the survey results with the Healthcare Organisation. They are processing the personal data on the Healthcare Organisation's instructions.

For more information on data controllers and data processors please see the DPC website

1.2 Data Processing Activity Details

This section relates to the details of the planned or proposed data processing activity. All parts to this section must be filled out before moving on to the next section.

You should use section 1.2 to attempt to describe the "journey" from the data subject's perspective. How is the personal data collected e.g. data subject completes an online web form, personal data is collected from existing data sources, etc. It may be useful to draw a data flow chart/diagram to show the journey of the personal data, systems involved, changes that may happen to the data and outputs created by using the data. This is a very useful tool to consider risks that the data may be exposed to at each point in the data processing lifecycle.

Special Note: Artificial Intelligence (AI) / Machine Learning (ML) related Health Research projects

If the proposed processing activity includes the use of machine learning or Artificial Intelligence algorithms or software. The same rules apply, but specific attention must be provided as follows:

- The **accountability principle** under data protection law means the controller is responsible for complying with the data protection principles and must be able to demonstrate this compliance. When procuring an AI system from a third party, it is important to agree who will be the controller, joint-controller, or processor. In some cases, you will take on the role of controller. This may be the case if you make decisions about what the target output of the model will be (i.e. what is being predicted or classified), or about what features will be used in the model. As the controller, you need some level of understanding of how the AI system works to comply with data protection principles. For example, you need to understand how the AI system makes a decision because you have an obligation to explain this to people. In some cases, you may be a joint controller with the third party supplying the AI system for example when you provide personal data to the AI company when they are training their models on your dataset and on your direction.
- The **transparency principle** applies; you must be able to clearly explain (in plain English) how the data will be processed, what data fields are being used, where they are being taken from (directly from service user, from historic data held by organisation) Are other personal data sources being used to enrich the dataset.
- The **data minimisation principle** applies in so far as you must be able to explain why each data field being processed is necessary to achieve the intended outcome.
- **Purpose limitation principle** also applies, if Artificial Intelligence software is being used, this must be clearly documented. Some AI software will use the data for other non-related purposes therefore breach the purpose limitation principle. E.g. ChatGPT etc.
- You need to consider the special treatment of special category or 'sensitive data and the limitation on **automated decisions**. You need to document if the decisions being made with the personal data are fully automated (e.g. AI/ML automates the final decision e.g. service user is excluded / referred for additional treatment without any human intervention) or there is a human assessing the results before any decisions are being made as they relate to the individuals whose data is being processed. (e.g. Results of AI/ML analysis highlighting

potential health condition, a clinician reviews the results and recommends that the individual see a GP or go to ED department etc.

- You need to also clarify how feasible the AI/ML model training is based on the size and complexity of the dataset you are training with
- For further reading please see The Impact of GDPR on artificial intelligence

Section 2 DPIA Threshold Assessment

This section will help you to determine whether data processing is likely to result in a high risk to the rights and freedoms of data subjects, meaning a DPIA is required.

The legal requirement for completing a DPIA is set out in Art. 35 GDPR – Data Protection Impact Assessment. Please complete the threshold assessment before moving on to the next section. If you answer "Yes" to two or more of the listed criteria, a DPIA is required. The more criteria that are met by the processing, the more likely it is to present a high risk to the rights and freedoms of data subjects. If you answer "Yes" to any question, you should get your local Information Governance, Privacy or DPO Office representative to review your assessment to ensure that the threshold assessment has been completed correctly.

Key points to note:

- Special categories of personal data would include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation etc.
- Vulnerable data subjects would include children, employees, patients, the elderly etc. This also concerns more *vulnerable* segments of the population requiring special protection, such as, for example, the mentally ill, asylum seekers, or the elderly, a patient lacking decision-making capacity, or in any case where an imbalance in the relationship between the position of the data subject and the controller can be identified.
- Data processing on a large scale would include processing involving a large volume of personal data relating to data subject, where it occurs over a large geographical area, or where a large number of individuals are affected.
- Matching or combining two or more datasets would include, for example, matching medical personal data relating to an individual with a non-medical dataset, e.g. a HR dataset.
- Systematic monitoring would include, for example, collecting patient related data at a hospital level to understand bed occupancy, or the use of CCTV to observe data subjects in a particular area.
- Evaluation or scoring, including profiling data subjects would include personal data relating to a data subject's economic situation, performance at work, profiling based on a data subject's home address, etc.
- Automated-decision making with legal or similar significant effect would include, for example, a recruitment aptitude test which uses pre-programmed algorithms and criteria leading to the exclusion or discrimination of data subjects.

- Innovative use or applying new technological or organisational solutions would include, for example, deploying the use of Machine Learning (Artificial Intelligence) or combining the use of biometric data (finger print and face recognition).

Key Definitions for this Section:

- **Data Subjects:** Service users, patients (the individuals who are the research participants), employees or other individuals that may interact with the Healthcare Organisation (e.g. patient's families, HSE, S38 or S39 or Tusla staff etc.)
- **Personal data**: Any information relating to an identified or identifiable living natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- **Special Category Data (including sensitive data):** Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
- **Vulnerable data subjects:** These categories of data subjects may be considered vulnerable due to the power imbalance between the position of the data subject and the Healthcare Organisation as a public authority. Vulnerable data subjects may include children, employees, patients, the elderly etc.
- **Processing which is Large Scale, extensive or has long lasting effects:** While this should be considered on an individual basis for each DPIA based on the sensitivity of the data being processed, consider a threshold of 1000+ records relating to data subjects as large scale. If the processing involves less than 1000 records but you consider the data highly sensitive in nature (special category data including health records), you should still consider this as large scale processing.

Section 3 Details of the Data Processing Activity

3.1 Assessment of the Necessity and Proportionality of the Processing

The assessment of the necessity and proportionality of the processing is a DPIA requirement under Article 35 GDPR. All boxes should be filled in before moving on to the next section.

Lawful Basis

Please select which lawful bases under Article 6 and Article 9 of GDPR that are being relied upon for the processing of personal and special category data. For research related DPIAs you can speak to your Research Office, relevant local organisation or functional data protection support representative and / or Data Protection Officer (DPO) for advice if needed.

- **Consent (Article 6(1)(a) GDPR):** Consent is the lawful basis with which both data subjects and controllers are most familiar, however, this does not make it a more appropriate legal basis than any other. There are requirements and obligations attached to the reliance on consent as a legal basis for processing personal data. One of the conditions for consent under Article

7 of the GDPR is that consent must be '**freely given**'. Consent would not be regarded as freely given where there is a **clear imbalance** between the individual and the data controller, for example between a citizen and a public body, such as the HSE. For this reason consent is not an appropriate lawful basis for the HSE to rely on.

- **Contract (Article 6(1)(b) GDPR):** This lawful basis is utilised in contexts where there is a contractual relationship between the data subject and the controller, for example, where an individual becomes an employee of the HSE. To rely on this legal basis, the processing must be '**necessary for the performance'** of the contract. Additionally, this legal basis can only apply to contracts **between the actual data subject and the controller,** and not to processing of personal data for the purpose of performing a contract between a controller and a third party.
- **Legal obligation (Article 6(1)(c) GDPR):** This lawful basis is likely to be appropriate where controllers are obliged to process personal data to comply with legislation. For example, the HSE may be required to process notifications of positive Covid-19 cases or other infectious diseases in order to comply with the Infectious Diseases Regulations.
- **Vital interests (Article 6(1)(d) GDPR):** This lawful basis is likely to be appropriate where the processing of personal data is required in order to **protect someone's life,** or to mitigate against a serious threat to a person, for example a child or a missing person. This is sometimes relied on as a lawful basis for processing data by the HSE, for example where paramedics are required to process data relating to an individual who is seriously ill, unconscious, etc.
- **Public interest (Article 6(1)(e) GDPR):** This is the most common lawful basis relied upon by the HSE in the context of the provision of healthcare services. This lawful basis is appropriate where the processing is necessary for the performance of a task carried out in the public interest or in the **exercise of official authority vested in the controller.** The official authority vested in the HSE is set out in Section 7 of the Health Act 2004, i.e. to manage and deliver health and personal social services and to integrate the delivery of health and personal social services.
- **Legitimate interests (Article 6(1)(f) GDPR):** This lawful basis is likely to be an appropriate lawful basis where controllers process data subjects' personal data in a way which they would **reasonably expect** and which would have a minimal impact on their privacy, by virtue of the nature of the processing or safeguards introduced. Article 6(1) GDPR specifically **restricts public authorities,** such as the HSE, from relying on legitimate interests if they are processing data 'in the **performance of their tasks'.** The HSE may rely on this lawful basis for ancillary purposes such as office management, or other activities not related to the performance of its tasks as a healthcare provider.

<u>Key points to note:</u>

- The healthcare Organisation / data controller should not be relying on consent to process personal data for general processing activities relating to healthcare services provided by the healthcare Organisation.
- If the processing activity relates to the provision of healthcare services the most common lawful basis relied upon is Article 6(1)(e) for processing personal data.
- If the processing activity relates to the provision of healthcare services the most common lawful basis relied upon is Article 9(2)(h) for processing special category data, e.g. health data. *("Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services*

on the basis of Union or Member State law or pursuant to contract with a health professional…")

- If the processing activity relates to healthcare research the most common lawful basis relied upon is Article 9(2)(j) for processing special category data, e.g. health data. *processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.*
- Healthcare workers can be regarded as professional bound to professional secrecy see Data Protection Act 2018, Section 52 (irishstatutebook.ie) and definition of Healthcare workers can be found Health Identifiers Act 2014, Section 2 (irishstatutebook.ie)
- Article 6(1)(f) *legitimate interests* shall not apply to processing carried out by public authorities, such as the Healthcare Organisation, in the performance of their tasks.

3.3 Location of Data Processing

This section relates to the location of data processing and whether it will occur outside of the European Economic Area (EEA) or not.

Key definitions for this Section:

- **Third countries:** A country, which is not bound by the GDPR – as opposed to the 28 Member States of the EU, and the three European Economic Area (EEA) countries.
- **Adequacy decision:** A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.
- **Standard Contractual Clauses (SCCs):** Please see Art. 46 GDPR – Transfers subject to appropriate safeguards - General Data Protection Regulation (GDPR) (gdpr-info.eu)

Section 4 Data Protection Principles

This section relates to the data protection principles set out in Article 5 of the GDPR. Adherence to these principles is key for ensuring GDPR compliance, and to minimise data protection risks associated with the projects or activity. All parts to this section must be filled out before moving on to the next section. Non - compliance with these principles will be highlighted as risks or issues and may need to be rectified or mitigated prior to the processing activity commencing.

- **4.1 Lawfulness, Fairness and Transparency:** Under Article 5(1)(a), personal data shall be 'processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'). HSE privacy notices can be found online at GDPR Information - HSE.ie and may be useful as examples if your processing activity requires the creation of a privacy notice.
- **4.2 Purpose Limitation:** Under Article 5(1)(b), personal data shall be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific

or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not to be considered to be incompatible with the initial purposes ('purpose limitation').

- **4.3 Data Minimisation:** Under Article 5(1)(c), personal data shall be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed('data minimisation').
- **4.4 Accuracy:** Under Article 5(1)(d), personal data shall be 'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy').
- **4.5 Storage Limitation:** Under Article 5(1)(e), personal data shall be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed ('storage limitation').
- **4.6 Integrity and Confidentiality (Security):** Under Article 5(1)(f), personal data shall be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical and organisational measures ('integrity and confidentiality').
- **4.7 Accountability:** Under Article 5(2). The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). Accountability is an over-arching principle that the controller can demonstrate compliance with the data protection principles.

4.8 Further Measures (Definitions of Anonymisation / Pseudonymisation)

- **Anonymisation:** Individuals are no longer directly or indirectly identifiable from a dataset. Where data has been anonymised, the original information should be securely deleted to prevent any reversing of the 'anonymisation' process. In most cases, if this deletion does not take place then the data is classified as 'pseudonymised' rather than 'anonymised', and is still considered personal data.

- **Pseudonymisation:** The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Section 5 Data Subject Rights

This section relates to the rights of data subjects in relation to the processing of their personal data. In this section you should answer yes/no as to whether data subjects have been notified of how to exercise each of their rights. You should also document the method of how you informed them. This is usually done by way of privacy notice or patient information leaflet. If data subjects have not been informed you should document the reasons why.

Section 6 D – DPIA Management

Please ensure that all processing of personal and special category data from this DPIA has been included in the site Records of Processing Activity (RoPA)

Section 7 DPO Opinion

This section will be completed by the DDPO / DPO Office or relevant Data Protection Review Resource once the DPIA has been submitted and reviewed.

Section 8 Approval

This section relates to the outcome of the DPIA process. The DPIA owner is responsible for accepting the risks associated with the processing activity.

Review & Sign-off

Project Sponsor shall sign finalised web form once Final DPO opinion has been provided.

Revision History

Version	Changes Made	Reviewed by	Approved by
1.0	New document.	**Name: Mark Foy** **Title:** DPO Support **Name:** Róisín Bradley **Title:** Legal Contract Reviewer, HSE **Name:** Tom Cochrane & Adam Hanlon **Title:** Legal Advisers	**Name: Mary Deasy** **Title:** HSE National Data Protection Officer **Name: Johnny Farren** **Title** DPO Support **Name: Racheal Batten** **Title:** National Lead for Legal Support and Data Protection

Document Statement

This document has been developed by the HSE, working with the Department of Health, the Voluntary Hospital Group, Universities, Clinical Research Organisations and Health Research Data Protection Network Group. It has been issued in conjunction with existing Healthcare Organisation policies, procedures, protocols, guidelines, education and training programmes. The HSE requests that no part of this publication be externally reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) without an acknowledgement of the source of the material which, in addition, should be included in all references.