**Health Research**

**Data Protection Impact Assessment Form**



# Document Information

|  |  |
| --- | --- |
| Title | Health Research Data Protection Impact Assessment (DPIA) Form |
| Purpose | A DPIA is a process to help identify and minimise the data protection risks of a project or activity, and will help assess and demonstrate compliance with data protection obligations. While it is prepared by those involved in the project, its intended audience is the public. Accordingly, it should be drafted with that audience in mind in terms of being as easy to read as possible.  |
| Scope |  DPIA for Health Research processing activities |
| Version | 7.0  |

[Data Protection Officer and Deputy Data Protection Officer Contact Details](https://www.hse.ie/eng/gdpr/data-requests/Data-%20Protection%20Officer%20and%20Deputy%20Data-Protection%20Officer%20contact%20details)

# Section A - DPIA Ownership

|  |  |
| --- | --- |
| Project Title |  |
| Type of project i.e., technology, admin, research, clinical audit |  |
| Explain broadly what the study involves and aims to achieve. You may find it helpful to refer or link to other study documents here (e.g. Participant Information Leaflet, Study Protocol etc). |  |
| Duration of project / processing activity |  |
| Name and title of person completing this form: |  |
| Contact detailsPhone:Email: |  |
| Service area: |  |
| Project sponsor: |  |
| This DPIA will be kept under review by: |  |

**Health Research Study Details**

|  |  |
| --- | --- |
| **Question** | **Response** |
| What is the study number (CTRIAL-IE NO. [INSERT]; EUDRACT NO. [INSERT] OR Other Registry Identifier(s), e.g. clinicaltrials.gov) associated with the research? |  |
| What is the study name/full title? |  |
| What type of study is being carried out? (tick all that apply) |

|  |  |
| --- | --- |
| [ ]  Clinical Trial (IMP)[ ]  Performance Studies of medical devices[ ]  Clinical Investigation of medical devices[ ]  Research Study | [ ]  Prospective research[ ]  Retrospective Chart review research(see section 6.8 of [HSE Consent Policy)](https://assets.hse.ie/media/documents/ncr/HSE-National-Policy-for-Consent-in-Health-and-Social-Care-Research-compressed.pdf)[ ]  Other (please specify) for example Research that may re-identify individuals? Data registry, or biobank establishment etc.: |
|  |  |
| Who is the Study Sponsor? |  |
| Who is the Chief Investigator (or National Lead Investigator) Name/Institution? |  |

Brief description of the study including the study background and need for the study (objectives, benefits, etc.): |
| Is this a study in a rare disease/condition? |

|  |  |
| --- | --- |
| ☐ Yes | ☐ No |
| If yes, specify:  |  |

 |
| What is the anticipated study start date? |  |
| What is the anticipated study end date? |  |

# Description of the Data Processing Activity

## Parties to the processing

The **Data controller** is the organisation (Healthcare, University, Pharma etc.) which (either alone or with others) determines the purposes and means for the collection and processing of personal data. The data controller decides ‘why’ and ‘how’ the personal data is processed. Control, rather than possession, of personal data is the key factor. Where two organisations jointly determine the purposes and means for processing the personal data, both organisations are joint controllers.

Data controllers and data processors must be legal entities. Accordingly, for example even if several Healthcare Organisation departments are involved with the processing activity, it is the organisation and not the department that is the controller or processor.

Data processors work under the instruction of the data controller, e.g. an IT Service provider acting as processor provide the technical infrastructure for Healthcare Organisation to communicate by email, share documents, data etc.

|  |  |
| --- | --- |
| **Question** | **Response** |
| Who is the data controller? If there is more than one data controller, please identify and specify whether they are joint controllers or a series of independent controllers and outline their role and responsibility in the processing activity?  |  |
| If there is more than one data controller, has a data sharing agreement (or joint controller agreement) been signed and put in place?  |  |
| Please list the relevant Healthcare Organisation departments involved in the processing activity. |  |
| Who is the data processor / are the data processors and what is their role and responsibility in the processing activity?  |  |
| Are there any data sub-processors and if so, what is their role and responsibility in the processing activity? |  |
| For any data processor involved, has a data processing agreement been signed and put in place (or in the process of being arranged)? |  |
| Is the personal data going to be shared with anyone other than the listed data controllers/processors? If yes, list the recipients of the personal data and for what purpose it is being shared.  |  |

## Data Processing Activity Details

|  |  |
| --- | --- |
| **Question** | **Response** |
| Title of the activity: |  |
| Provide a detailed description of the process describing the “customer journey” and lifecycle of the data (where is the personal data sourced from, how is it collected, amended, stored, and ultimately destroyed or de-identified etc.): |  |
| Please provide details of where the data will be stored. Please explain exactly the location of where the information being processed / stored. For example: Server in a Data centre in Ireland, Cloud provider (AWS in Netherlands), desktop / pc of Researcher in University X, paper files in secure room in x Hospital. (Refer to section 3.3 below for geographical Location). Please consider and document if and where the data is stored if in a variety of locations at different stages of the project. |  |
| **Data Flow Description (or provide diagram):** Please describe the dataflow detailing how the specific data fields are collected, amended, enriched, and processed at each stage as well as the systems involved. |
| **Question** | **Response** |
| Who are the data subjects whose data will be processed? |  |
| How is the data accessed and used and by whom? |  |
| How long do you intend to keep the data for?Please provide the clinical, operational or legal requirement to justify the length of time data will be retained. |  |

**Data Table**

| **Data item** | **Yes** | **Specify why each applicable data item will be collected, used and/or processed?** |
| --- | --- | --- |
| First Name |[ ]   |
| Last Name | [ ]   |  |
| Initials | [ ]  |  |
| Phone Number (Mobile / Landline) | [ ]  |  |
| email address | [ ]  |  |
| Postal address (house number, street, town, Eircode etc.) | [ ]  |  |
| Truncated Eircode | [ ]  |  |
| IMEI number (International Mobile Equipment Identity. It’s a unique number for identifying a device on a mobile network. | [ ]  |  |
| IP address | [ ]  |  |
| Date of Birth | [ ]  |  |
| Age Range  | [ ]  |  |
| Partial date of birth |[ ]   |
| Medical Record no. | [ ]  |  |
| Staff Number |[ ]   |
| PPSN  |[ ]   |
| Government Issue ID number (Passport, driver’s license, PSC) |[ ]   |
| Country of Birth |[ ]   |
| Citizenship |[ ]   |
| Religious or philosophical beliefs |[ ]   |
| Social Media Profile |[ ]   |
| Sex (male / female) | [ ]   |  |
| Gender | [ ]  |  |
| Racial/Ethnic Origin | [ ]  |  |
| Sexual Orientation | [ ]  |  |
| Genetic data | [ ]  |  |
| Biometric data | [ ]  |  |
| Health Data | [ ]  |  |
| Medical History | [ ]  |  |
| Family Medical History | [ ]  |  |
| Biological Samples (Please provide details) | [ ]  |  |
| Test Results | [ ]  |  |
| Trial Treatments | [ ]  |  |
| Adverse Event Descriptions | [ ]  |  |
| Disease Course | [ ]  |  |
| Trade Union Membership | [ ]  |  |
| Data Related to minors | [ ]  |  |
| Other Demographics (e.g., marital status, income, profession, homeless etc.) | [ ]  |  |
| Lifestyle/ social circumstances | [ ]  |  |
| *Other, specify* |[ ]   |

# DPIA Threshold Assessment

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

**If you answer “Yes” to two or more of the below 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 the threshold assessment has been completed correctly.

Please mark “Yes” or “No” for each of the following:

**Does your processing activity involve:**

|  |  |
| --- | --- |
| 1. **The use of personal data, including sensitive or** special categories of data (e.g., health data, ethnicity, etc.).
 | Yes [ ] No [ ]  |
| 1. **Data concerning vulnerable data subjects,** e.g., children, employees, patients, the elderly etc.
 | Yes [ ] No [ ]  |
| 1. **Data processing on a large scale, extensive or has long-lasting effects**.For example where it involves 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.
 | Yes [ ] No [ ]  |
| 1. **Matching or combining two or more datasets,** e.g. enriching the datasets using additional data sources to provide further information regarding the individuals in the study
 | Yes [ ] No [ ]  |
| 1. **Systematic monitoring:** processing used to observe, monitor or control data subjects, including data collected through systematic monitoring of a publicly accessible area e.g., collecting patient related data at the hospital level to understand bed occupancy, or CCTV.
 | Yes [ ] No [ ]  |
| 1. **Evaluation or scoring,** including profiling data subjects, e.g. based on a data subject’s economic situation or performance at work.
 |  |
| 1. **Automated-decision making with legal or similar significant effect,** e.g. a recruitment aptitude test which uses pre-programmed algorithms and criteria leading to the exclusion or discrimination of individuals.
 | Yes [ ] No [ ]  |
| 1. **Innovative use or applying new technological or organisational solutions,** such as Machine Learning (Artificial Intelligence) or combining use of biometric (finger print and face recognition).
 | Yes [ ] No [ ]  |

# Details of the Data Processing Activity

## Assessment of the necessity and proportionality of the processing

|  |  |
| --- | --- |
| **Question** | **Response** |
| What the benefits of the data processing activity are to: (i) organisation(s) involved, (ii) data subjects involved, (iii) the health system or society (that is, does this processing activity have a public interest perspective)? | (i):(ii):(iii) |
| Can you achieve the intended outcome of the project using less personal data or without using personal data at all? Explain your considerations in arriving at the answer.  |  |

## Lawful basis

|  |  |
| --- | --- |
| **Question** | **Response** |
| Please cite the legislation and specific sections (chapter, article, and paragraph) of legislation which underpin the lawful basis for this processing activity. |  |
| What is the lawful basis for processing personal data under GDPR Article 6(1)? | [ ]  (a) Consent from the data subject. [ ]  (b) Processing is necessary for the performance of a contract.[ ]  (c) Processing is necessary for compliance with a legal obligation.[ ]  (d) Processing is necessary to protect the vital interests of the data subject. [ ]  (e) Processing is necessary for the performance of a task carried out in the public interest, in the area of public health or in the exercise of official authority vested in the controller.[ ] (f) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party. |
| If you are processing special category data you should also satisfy what the lawful basis for processing is under GDPR Article 9(2).  | [ ]  (a) Explicit consent from the data subject.[ ]  (b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law.[ ]  (c) Processing is necessary to protect the vital interests of the data subject or of another natural person. [ ]  (d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim.[ ]  (e) Processing relates to personal data which are manifestly made public by the data subject.[ ]  (f) Processing is necessary for the establishment, exercise or defence of legal claims.[ ]  (g) Processing is necessary for reasons of substantial public interest.[ ]  (h) 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 or services.[ ]  (i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.[ ]  (j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes |
| Special Category or sensitive data referred above may be processed for the purposes referred to in point (h) above when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy. Can you confirm that the individual processing the data is a professional subject ([e.g. healthcare worke](https://www.irishstatutebook.ie/eli/2014/act/15/section/2/enacted/en/html)r) bound by the obligation of professional secrecy? | [ ]  Yes[ ]  No |

##  Location of data processing

|  |  |
| --- | --- |
| **Question** | **Response** |
| Where the data is originally located and where is it subsequently processed and stored? |  |
| Single or multi-site and Countries involved:(If Third country site, please insert where appropriate) |

|  |  |  |
| --- | --- | --- |
| [ ]  Ireland | [ ]  Single site | [ ]  Multi-site |
| [ ]  EU/EEA sites | [ ]  Single site | [ ]  Multi-site |
| [ ]  Third country sitesThird Country: | [ ]  Single site | [ ]  Multi-site |

 |
| If the data is transferred outside the EU / European Economic Area (EEA), list the recipient countries. |  |
| Please confirm that the details of international transfers outside the EU / European Economic Area (EEA) are communicated clearly in the Patient Information leaflet. |  |
| Please confirm that a Transfer Impact Assessment has been carried out for all instances of transfers to third countries outside the EU/EEA and where there is no adequacy decision. (See [Adequacy decisions (europa.eu)](https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en)) |  |
|  If data is being transferred outside EU/EEA, is an adequacy decision in place for the third country?  |  |
| If no adequacy decision is in place, have Standard Contractual Clauses (SCCs) been added to the contract / what other transfer mechanism is in place? Binding Corporate Rules, etc. (Please provide details in box opposite)  | [ ]  on the basis of an Adequacy Decision,[ ]  using the safeguard of Standard Data Protection clauses, [ ] using the safeguard of Binding Corporate Rules, [ ]  on the basis of approved Codes of Conduct, [ ]  on the basis of approved Certification Mechanisms, [ ] on the basis of a legally binding and enforceable instrument between public authorities or bodies,[ ]  on the basis of a Derogation |

# Data protection principles

## 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’).*

|  |  |
| --- | --- |
| **Question** | **Response** |
| Is there a privacy notice or patient/participant information leaflet (PIL) presented to data subjects involved that informs them of the data processing activity?Please provide a copy of the privacy notice / PIL as well as or other means by which data subjects are informed of data processing (eg posters, website etc). |  |
| Have data subjects involved or representative groups been consulted about the data processing activity? If yes, state the number of individuals, or details of representative groups consulted, method of consultation and describe the outcome of the consultation.If no, explain the reason for not consulting. |  |
| Surprise test: Would data subjects involved be surprised if they knew their data was being processed in this way? |  |
| **Identify and assess data protection risks:** considering this data protection principle, describe source of risk and nature of potential impact on individuals. *(Please note: Likelihood x Impact = Overall Rating)* | **Likelihood (1-5)** | **Impact (1-5)** | **Overall (1-25)** |
| **1).**  |  |  |  |
| **Identify measure of mitigate data protection risks:** Identify measure that can be put in place to reduce or eliminate risks identified above. What is the residual risk following the implementation of measures to reduce the risk of this DP Principle.  | **Describe Effect on Risk (Eliminated or reduced)** | **Residual risk rating (1-25)** | **Status of mitigation action** |
| **1.)** |  |  |  |

## 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*](https://gdpr-info.eu/art-89-gdpr/)*(1), not to be considered to be incompatible with the initial purposes (‘purpose limitation’).*

|  |  |
| --- | --- |
| **Question** | **Response** |
| How are you ensuring that you or other stakeholders involved aren’t using the data you collect for any other purpose than it was originally collected? (function creep) |  |
| **Identify and assess data protection risks:** considering this data protection principle, describe source of risk and nature of potential impact on individuals. *(Please note: Likelihood x Impact = Overall Rating)* | **Likelihood (1-5)** | **Impact (1-5)** | **Overall (1-25)** |
| **1).** |  |  |  |
| **Identify measure of mitigate data protection risks:** Identify measure that can be put in place to reduce or eliminate risks identified above. What is the residual risk following the implementation of measures to reduce the risk of this DP Principle.  | **Describe Effect on Risk (Eliminated or reduced)** | **Residual risk rating (1-25)** | **Status of mitigation action** |
| **1.)** |  |  |  |

## 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’).*

|  |  |
| --- | --- |
| **Question** | **Response** |
| How are you ensuring that you are not collecting any more data than is required for your processing activity? E.g., do you need the name and address of the patients or service users to achieve the outcome of this processing activity? Any personal data in any format needs to be assessed for minimisation for example hand written survey responses, audio or video files containing personal data should be destroyed once text is transcribed. |  |
| **Identify and assess data protection risks:** considering this data protection principle, describe source of risk and nature of potential impact on individuals. *(Please note: Likelihood x Impact = Overall Rating)* | **Likelihood (1-5)** | **Impact (1-5)** | **Overall (1-25)** |
| **1).** |  |  |  |
| **Identify measure of mitigate data protection risks:** Identify measure that can be put in place to reduce or eliminate risks identified above. What is the residual risk following the implementation of measures to reduce the risk of this DP Principle.  | **Describe Effect on Risk (Eliminated or reduced)** | **Residual risk rating (1-25)** | **Status of mitigation action** |
| **1.)** |  |  |  |

## 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’).*

|  |  |
| --- | --- |
| **Question** | **Response** |
| What controls do you have in place to ensure the data is kept up to date and accurate? Either at point of collection or during the different data processing stages. |  |
| **Identify and assess data protection risks:** considering this data protection principle, describe source of risk and nature of potential impact on individuals. *(Please note: Likelihood x Impact = Overall Rating)* | **Likelihood (1-5)** | **Impact (1-5)** | **Overall (1-25)** |
| **1).** |  |  |  |
| **Identify measure of mitigate data protection risks:** Identify measure that can be put in place to reduce or eliminate risks identified above. What is the residual risk following the implementation of measures to reduce the risk of this DP Principle.  | **Describe Effect on Risk (Eliminated or reduced)** | **Residual risk rating (1-25)** | **Status of mitigation action** |
| **1.)** |  |  |  |

## 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’).*

|  |  |
| --- | --- |
| **Question** | **Response** |
| Have you designed the ability to delete data when no longer required? Please describe in detail how long this data will be kept for, why and also how this data will be deleted when no longer required (how, why when, who) |  |
| How are you monitoring the retention of data to ensure it aligns Research Ethic Committee approval or HSE Record Retention Policy (if covered)? |  |
| **Identify and assess data protection risks:** considering this data protection principle, describe source of risk and nature of potential impact on individuals. *(Please note: Likelihood x Impact = Overall Rating)* | **Likelihood (1-5)** | **Impact (1-5)** | **Overall (1-25)** |
| **1).** |  |  |  |
| **Identify measure of mitigate data protection risks:** Identify measure that can be put in place to reduce or eliminate risks identified above. What is the residual risk following the implementation of measures to reduce the risk of this DP Principle.  | **Describe Effect on Risk (Eliminated or reduced)** | **Residual risk rating (1-25)** | **Status of mitigation action** |
| **1.)** |  |  |  |

## 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’).*

|  |  |
| --- | --- |
| **Question** | **Response** |
| What technical and organisational measures have been put in place to ensure security of data? (e.g. secure rooms, cabinets, passcodes etc.) |  |
| How is the data securely shared or transferred? (e.g., courier, email, password protected, ShareFile, encrypted, SFTP, etc.) |  |
| For any data processor where there is a direct connection to the Data Controller Organisation network or transfer of data to the processor, have ICT Security assessed the technical and organisational security measures? An IT security questionnaire may be required:[hse-supplier-it-security-assessment-questionnaire.docx](https://scanner.topsec.com/?d=2120&r=show&u=https%3A%2F%2Fview.officeapps.live.com%2Fop%2Fview.aspx%3Fsrc%3Dhttps%253A%252F%252Fhealthservice.hse.ie%252Ffilelibrary%252Fstaff%252Fhse-supplier-it-security-assessment-questionnaire.docx%26wdOrigin%3DBROWSELINK&t=06d94049f8728f1ae2f6288aa824ef76aac76e18)  |  |
| **Identify and assess data protection risks:** considering this data protection principle, describe source of risk and nature of potential impact on individuals. *(Please note: Likelihood x Impact = Overall Rating)* | **Likelihood (1-5)** | **Impact (1-5)** | **Overall (1-25)** |
| **1).** |  |  |  |
| **Identify measure of mitigate data protection risks:** Identify measure that can be put in place to reduce or eliminate risks identified above. What is the residual risk following the implementation of measures to reduce the risk of this DP Principle.  | **Describe Effect on Risk (Eliminated or reduced)** | **Residual risk rating (1-25)** | **Status of mitigation action** |
| **1.)** |  |  |  |

## 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.

|  |  |
| --- | --- |
| **Question** | **Response** |
| For any risks highlighted in this DPIA, what remedial plans have you put in place and have they been assigned to anybody? |  |
| **Identify and assess data protection risks:** considering this data protection principle, describe source of risk and nature of potential impact on individuals. *(Please note: Likelihood x Impact = Overall Rating)* | **Likelihood (1-5)** | **Impact (1-5)** | **Overall (1-25)** |
| **1).** |  |  |  |
| **Identify measure of mitigate data protection risks:** Identify measure that can be put in place to reduce or eliminate risks identified above. What is the residual risk following the implementation of measures to reduce the risk of this DP Principle.  | **Describe Effect on Risk (Eliminated or reduced)** | **Residual risk rating (1-25)** | **Status of mitigation action** |
| **1.)** |  |  |  |

## Further Measures

 **Anonymisation / Pseudonymisation**

|  |  |
| --- | --- |
| **Question** | **Response**  |
| Describe if the data collected and processed for the study will be identifiable, pseudonymised, and/or anonymised including who will pseudonymise/ anonymise data and who will have access to each type of data for example written, electronic, audio/video recordings, photographs? |  |
| Identifiable data (*specify who will hold the data, how it will be held, where, who will have access etc)*: |  |
| Pseudonymised data *(also specify who will hold the key, how it will be held, where, etc.)*: |  |
| Anonymised data(*specify who will hold the data, how it will be held, where, who will have access etc)*: |  |
| Describe in detail any additional risks if the data collected and processed for the study will be identifiable, pseudonymised, and/or anonymised including who will pseudonymise/ anonymise data and who will have access to each type of data?Please attach any relevant documents pertaining to the process of pseudonymisation and/or anonymisation of data  |  |
| **Identify and assess data protection risks:** considering this data protection principle, describe source of risk and nature of potential impact on individuals. *(Please note: Likelihood x Impact = Overall Rating)* | **Likelihood (1-5)** | **Impact (1-5)** | **Overall (1-25)** |
| **1).** |  |  |  |
| **Identify measure of mitigate data protection risks:** Identify measure that can be put in place to reduce or eliminate risks identified above. What is the residual risk following the implementation of measures to reduce the risk of this DP Principle.  | **Describe Effect on Risk (Eliminated or reduced)** | **Residual risk rating (1-25)** | **Status of mitigation action** |
| **1.)** |  |  |  |

## Requirements for Explicit Consent for Research

|  |
| --- |
| **Health Research Regulations - Explicit Consent required for Health Research** |
| In addition to satisfying Articles 6 & 9 GDPR requirements, have you obtained explicit consent for processing personal data for health research purposes? This 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) as amended in the 2002 Amending Regulations. |  |
| Describe how you will 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. |  |
| You must have a procedure in place if an individual wishes to withdraw their consent. Please outline the procedure. |  |
| Have you been provided with / or applied for a consent declaration or waiver for the processing of personal data from the [HRDC](http://www.hrcdc.ie)? If so, please provide details. |  |
| **Pre-screening** i.e. reviewing the personal data of an individual in order to assess whether they would be suitable or eligible for inclusion in a health research study. Must meet the following criteria: * Study carried out by either:
	+ a health practitioner employed by the Data Controller;
	+ a person studying to be a health practitioner who is under the direction and control of the Data Controller

There must be notices relating to the research on display in public areas of the controller’s organisation where individuals attend for provision of health care   |  |
| **Retrospective Chart Review** i.e. a type of research design in which pre-recorded, patient data are used to answer a research question. Must meet the following criteria:  * Study is low risk
* Study has been approved by a research ethics committee
* Study is carried out by either:
	+ a health practitioner employed by the Data Controller or
	+ a person studying to be a health practitioner who is under the direction and control of the Data Controller

There must be notices on display in public areas of the controller’s organisation where individuals attend for provision of health care   |  |
| Please see guide notes on Retrospective Chart review: [Guidance on Retrospective Chart Review](https://hrcdc.ie/wp-content/uploads/2021/01/3.-Guidance-on-Retrospective-Chart-Review-Amendments-Jan-2021.pdf) |

# Data Subject Rights

|  |  |
| --- | --- |
| **Question** | **Response** |
| Describe what arrangements have been put in place by the research team to facilitate data subjects exercising their rights under data protection law.  |  |
| Have data subjects been notified of how to exercise their right to:* Fair and lawful processing
* Access
* Rectification
* Erasure (‘right to be forgotten’)
* Restriction of processing
* Data portability
* Object to data processing
* Not be subject to automated profiling?
 | Yes [ ] No [ ]  |
| How have you notified data subjects of these rights? |  |

# Admin Section

**A – Investigator details**

|  |
| --- |
| **INVESTIGATOR SITE DETAILS*****Enter details of all sites involved in the study*** ***(copy and paste the following table and divider line for each additional site)*** |
| Chief/Principle Investigator Name:  |  |
| Authorised individual:  | ☐ Yes☐ NoIf No please explain why not: |
| Institution:  |  |
| Address: |  |
| Site no.: |  |
| Contact tel. no.: |  |
| Email address: |  |
|  |

**B – Supporting Documents**

|  |
| --- |
| **SUPPORTING DOCUMENTS** |
| **Document name** | **Version no./date or identifier** |
| *e.g. Informed consent/ assent form* | *e.g. 1/ dd-Mon-yyyy* |
| e.g. Patient Information leaflet/ Privacy notices | *e.g. 1/ dd-Mon-yyyy* |
| e.g. Deferred consent/consent to continue form |  |
| e.g. Data Sharing / Processing Agreements |  |
| e.g. Information Security Assessments |  |

**C – Study Sponsor Review & Sign-Off**

|  |
| --- |
| **To be completed by Site Study Sponsor:** |
| Name: | Date: |
| Title: | Signature: |
| **D – DPIA Management** |  |
| **DPIA Administration** |
| Will the data processed in this activity be used for any other purpose in the future e.g., reporting, analysis, research? If data will be used for any other purpose the DPIA will need to be updated. |  |
| This DPIA will be kept under review by: |  |
| Scheduled review date |  |
| 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) |  |
|  |

# DPO (or Designated Data Protection Lead/Representative) Opinion

# Approval

*To be completed by the business/project lead for the processing activity on behalf of the data controller*

**Outcome:**

Approved [ ] 

Denied [ ] 

DPC Consultation Needed [ ] 

**Please ensure you provide the DPO with final signed DPIA for organisation records.**

**Signed:**

**Date:**