 *[](https://www.google.ie/url?sa=i&url=http://www.nuigalway.ie/&psig=AOvVaw08TUFAowPR3vzU_G5bx6H6&ust=1578674898023000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCJiulLb89uYCFQAAAAAdAAAAABAE)*

Saolta-NUI Galway Clinical Research & Development Office

*Oifig Taighde agus Forbartha Cliniciúil*

CRDO…….*FOSTERING AN ENVIRONMENT OF SAFE, QUALITY, AND INNOVATIVE RESEARCH FOR ALL.*

**Health Research Regulations and your responsibility as a Research Investigator**

* All researchers should be aware of the GDPR and Department of Health Regulations and how they can impact on your proposed research.
* Health Research is currently regulated by:

1. General Data Protection Regulation 2016
2. Data Protection Act 2018
3. Health Research Regulations 2018

**GDPR:**

* GDPR came into effect throughout the EU on the 25th May 2018. It has a significant impact on how research is conducted. GDPR governs the collection, use and storage of all personal data of living individuals.
* GDPR has data protection principles similar to the principles set out in the 1995 Data Protection Directive:

Fairness

Lawfulness and transparency

Purpose limitation

Data minimisation

Data quality

Security

Integrity

Confidentiality

* A new accountability principle makes controllers responsible for demonstrating compliance with the data protection principles.
* The following are some of the significant changes in the GDPR regulations:
* Consent – The GDPR requires consent to be unambiguous.
* Transparency - Data subject must know how and why their data is being used.
* Children and consent – verifiable parental consent is required for use of a child’s personal data.
* Regulated data – the definition of “Personal Data” and “Sensitive Data”. Sensitive data now includes genetic and biometric data.
* Pseudonymisation – is a privacy enhancing technique which allows processing of personal data in a way that it can no longer be attributed to the specific data subject without additional information, which is to be held separately and subject to safeguarding measures to ensure non-attribution.
* Personal Data Breach – a new security breach law is introduced for all data controllers.
* Data protection by design and accountability – organisations are required to adopt significant new technical and organisational measures to demonstrate their GDPR compliance.
* Enhanced rights – Data Subjects are given enhanced rights including the right to be forgotten, data portability rights and the right to object to automated decision making.
* Supervisory authorities and the European Data Protection Board – regulatory oversight of data protection will change significantly. The EDPB will have extensive powers to determine disputes between national supervisory bodies.

**GDPR considerations when conducting research**:

1. IDENTIFY THE DATA CONTROLLER & PROCESSOR
2. ROLE OF DATA PROTECTION OFFICER
3. KNOW YOUR DATA
4. KNOW YOUR LAWFUL BASIS FOR PROCESSING
5. BE TRANSPARENT
6. INFORM DATA SUBJECT OF THEIR RIGHTS
7. KNOW HOW TO HANDLE ACCESS REQUESTS
8. HOW TO TRANSFER PERSONAL DATA OUTSIDE EU
9. DATA BREACH REPORTING & SECURITY
10. FINES
11. RIGHT TO COMPENSATION
12. PERSONAL CRIMINAL LIABILITY

**IDENTIFY THE DATA CONTROLLER & PROCESSOR**

* A data controller determines the purposes, conditions, and means of the processing of personal data.
* There may be joint controllers or more than one controller.
* The **controller** is responsible for ensuring compliance with the principles of GDPR.
* In practice, to identify the data controller ask the following questions:
  + Who is deciding WHY (purpose) personal information is going to be processed? e.g. a study to investigate medication compliance.
  + Who is deciding HOW (means and conditions) the personal information is to be processed? e.g. the manner in which the research is going to be conducted. Project design.
* Your organisation is a joint controller if with one or more organisations you jointly determine WHY and HOW data should be processed.
* If your organisation is a joint controller your organisation must enter an agreement setting out responsibilities for complying with GDPR.
* A data processor processes personal data on behalf of the data controller.
* Examples of data processors include:
* payroll companies or accountants or similar who hold and process personal information on behalf of someone else;
* "cloud" providers are also generally data processors;
* If you hire a 3rd party to process data for your research (e.g. a transcription service to transcribe audio tapes of interviews) - the third party will be a data processor.
* A data processor **does not include** the employees of a Data Controller (e.g. researchers employed on research projects in which personal data is collected, processed and stored)
* If you are a researcher, you might be a data processor if you are employed on a **service contract** that collects, stores, or processes personal data on behalf of a Data Controller.

**ROLE OF DATA PROTECTION OFFICER**

* The controller & processor shall ensure the DPO is involved properly and in a timely manner, in all issues relating to data protection
* The DPO shall inform and advise the controller or processor of their legal obligations
* The DPO shall monitor compliance
* The DPO shall provide training and policies
* The DPO shall provide advice regarding Data Protection Impact Assessments. – SECTION 4 GDPR
* **Saolta HG DPO = Deputy Data Protection Officer West:** 091-775819 Email: [ddpo.west@hse.ie](mailto:ddpo.west@hse.ie)

**KNOW YOUR DATA**

* IDENTIFIABLE DATA- is the data subject identified.
* PSEUDONYMISED DATA- data that can no longer be attributed to the data subject without additional information which is kept separately.
* ANONYMOUS- data which can no longer be attributed to the data subject.
* Identifiable & pseudonymised data falls under GDPR.
* Anonymised data falls outside the scope of the GDPR.
* PERSONAL DATA- is any information that relates to an **identified or identifiable living individual**.
* Examples of personal data – NOT LIMTED TO THIS LIST:
* a name and surname
* a home address
* an email address
* an identification number
* a location number
* IP address
* data held by a hospital or doctor, which could be a symbol that could uniquely identify someone
* SENSITIVE PERSONAL DATA– data revealing:
* racial or ethnic origin
* religious or philosophical beliefs
* trade union membership
* genetic data
* **health data**
* biometric data
* data concerning sex life
* sexual orientation
* ‘GENETIC DATA’ includes data derived from biological samples from an individual, such as chromosomal or DNA.
* ‘BIOMETRIC DATA’ includes data derived from fingerprints and facial recognition.

**KNOW YOUR LAWFUL BASIS FOR PROCESSING**

* This is your valid legal reason to process and use data under GDPR.
* Article 6 – provides 6 legal basis for processing Personal Data.
* Article 9 – provides 10 legal basis for processing Sensitive Personal Data.
* You must pick one legal basis from Article 6 when processing personal data and an additional legal basis from Article 9 when processing sensitive personal data.
* You must have TWO legal basis for processing sensitive personal data.
* **Article 6 –Lawful Basis**
* For public authorities such as universities, HSE etc. the most relevant legal basis for research under Article 6 will be:
* Article 6(1)(e) Processing is necessary for the performance of a task carried out in the public interest.
* If using this you must document justification by referencing the public research purpose of the authority as established by charter or statute.
* **Article 9-Lawful Basis**
* Most health research will require the processing of sensitive personal data i.e. health data.
* The most relevant legal basis for research is Article 9(2)(j).
* Processing is necessary for scientific research purposes.
* If using -must have -safeguards to ensure data minimisation (pseudonymisation).

**BE TRANSPARENT**

* GDPR is all about being open with data subjects and informing them of how their data is to be used.
* The controller must inform/provide notice data subjects of what is being done with their data.
* Need to provide a Participant Information Leaflet or privacy notice.
* You must use clear, understandable language: concise, easily accessible, easy to understand, intelligible, age appropriate, clear and plain.
* Information Leaflet should contain the following:
  + the controller’s identity and contact information;
  + contact details of the data protection officer;
  + your legal basis for processing;
  + if processing under legitimate interest –state what that is;
  + the intended purposes of the processing activities;
  + where applicable, that the data will be transferred to another entity or to a third country;
  + information about any profiling (automated processing to evaluate aspects of that person such as work performance, behaviour, preferences) individuals will be subject to;
  + inform data subjects of the nature of the processing activities and the rights available to them;
  + recipients or categories of recipients of the data;
  + how long will data be stored for?
* Further processing/ secondary processing requires an updated notice or information if processing data for a different purpose.
* A researcher may be exempt from the notice requirement if they received the personal data from someone other than the data subject (e.g. BioBank).
* A researcher may also be exempt if the notice is “likely to render impossible or seriously impair the achievement of the research objectives”. There must be appropriate safeguards in place-minimisation of data such as pseudonymisation

**INFORM DATA SUBJECT OF THEIR RIGHTS**

* The controller, must inform the data subject of their right to:
  + Access
  + Rectification
  + Erasure
  + Restrict processing
  + Data portability
  + Object to processing
  + Lodge a complaint with the Data Protection Commissioner
* Exemptions to data subject rights as laid out in GDPR maintained by Regulation:
* Possibly rights of access, rectification, erasure, restriction of processing and objection to processing can be overridden if the request is likely to render impossible or seriously impair the achievement of the research objectives.

**KNOW HOW TO HANDLE ACCESS REQUESTS**

* The time period for dealing with requests is one month.
* No fee.
* The controller may charge a reasonable fee for further copies requested, or where access requests are manifestly unfounded or excessive.

**HOW TO TRANSFER PERSONAL DATA OUTSIDE EU**

* The GDPR allows transfer to non EU countries with “adequate level of protection” as determined by the European Commission.
* Specific safeguards, including **Binding Corporate Rules and standard contractual clauses**, or if the data subject has provided explicit consent.

**DATA BREACH REPORTING & SECURITY**

* Mandatory obligation to report data breaches to the Office of the Data Protection Commissioner.
* Within 72 hours where there is a risk to the rights of data subjects.
* Controllers have to notify data subjects where the breach is likely to result in a ‘high risk’ to them.

**FINES**

* Non-compliance subject to fines of up to €20 million or 4% of the total worldwide annual turnover of the preceding financial year.
* Fines can be imposed in addition to, or instead of, any corrective measures -such as warnings or reprimands.
* Fines of up to €10 million or 2% worldwide annual turnover for infringement of e.g. :
* Conditions of obtaining child’s consent;
* Data protection by design and default;
* Joint controller arrangements;
* Obligations of processors;
* Security measures;
* Notifications;
* Conducting DPIA.
* Fines up to €20 million or 4% total worldwide annual turnover for infringement of e.g. :
* Core data protection principles;
* Conditions for consent;
* Sensitive personal data processing;
* Data subject rights;
* Transfers outside EU;
* Obligations under Member State law (HRR).
  + Data Protection Act 2018: Public body fines limited to €1million

**RIGHT TO COMPENSATION**

* Data subjects can sue both controllers and processors for compensation for damage as a result of a breach of GDPR.
* Introduction of joint and several liability between parties engaged in the same data processing.
* Class actions.

**PERSONAL CRIMINAL LIABILITY**

* **Personal liability:**

• Consent

– must have known about the actions of the company;

–must have agreed to the action;

–can be established by inference.

* Connivance

–tacit agreement to the commission of the offence;

–aware of the commission of the offence;

–encompasses willful blindness to a course of action;

–can occur through reckless conduct by knowing of the risk but doing nothing about it.

* Neglect:

–failure to carry out a duty but without having actual knowledge of the offence committed;

–objective test that officer has fallen below an identifiable standard of action;

–neglect must have led to commission of the offence by the corporate.

* **OFFENCES**
* Knowingly or recklessly disclosing personal data without prior authority of controller/processor;
* Obtaining and disclosing personal data without prior authority of controller/processor;
* Selling personal data obtained and disclosed without prior authority controller/processor.
* See the following website for FAQ on GDPR for Health Researchers: <https://www.hrb.ie/funding/gdpr-guidance-for-researchers/general-gdpr-faq/>

**HEALTH RESEARCH REGULATIONS:**

* The Irish Government’s Data Protection Bill (2018) was enacted on the 24th of May 2018 and the Department of Health issued Regulations entitled Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018 on the 8th August 2018.
* The Health Research Regulations 2018 govern the use of personal data for health research purposes. These important new regulations outline mandatory [suitable and specific measures](http://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-health-research/suitable-and-specific-measures-for-health-research/)that ensure that health research in Ireland is conducted using best practice principles of information governance in line with new GDPR requirements. See the following website for FAQ on Health Research Regulations: <https://www.hrb.ie/funding/gdpr-guidance-for-researchers/health-research-regulations-2018/health-research-regulations-2018-faq/>
* The HRR provide the following **definitions** of Health Research:
* Research with the goal of understanding normal and abnormal functioning, at the molecular, cellular, organ system and whole body levels;
* Research that is specifically concerned with innovative strategies, devices, products or services for the diagnosis, treatment or prevention of human disease or injury;
* Research with the goal of improving the diagnosis and treatment (including the rehabilitation and palliation) of human disease and injury and of improving the health and quality of life of individuals;
* Research with the goal of improving the efficiency and effectiveness of health professionals and the health care system;
* Research with the goal of improving the health of the population or of defined sub-populations through a better understanding of the ways in which social, cultural, environmental, occupational and economic factors determine health status; & MAY include a necessary action taken to establish whether an individual may be suitable for inclusion in the research.
* Research is designed and conducted to generate new generalisable or transferable knowledge.
* It includes both quantitative and qualitative studies that aim to generate new hypotheses as well as studies that aim to test existing or new hypotheses.
* **RESEARCH IS NOT:**
* **Service evaluation**- assesses choices of treatment, care or services that are currently available according to guidance, professional standards and/or patient/service user preference.

e.g. evaluations performed to assess current care of a patient; evaluations of the standard of care a service achieves; evaluations aimed at determining or choosing appropriate treatment or service options.

* **Clinical Audit-**does this service reach a predetermined standard?
* It measures the delivery of an intervention against a standard.

e.g. evaluations designed to inform best service or care delivery; evaluations of whether or not a care or service meets required standards; evaluations relating to current treatments or interventions.

* **Usual practice -** “what are the health issues in this population and how do we address them?” or “what is the cause of this disease outbreak or incident and how do we manage it?”
* Usual practice may involve systematic, quantitative or qualitative methods. However, it assesses choices of intervention, treatment, care or services based on best public health evidence or professional consensus.
* It may involve analysis of existing routine data or administration of interview or questionnaire to those in the population of interest. It may involve a review of existing evidence.

**DATA CONTROLLER PROCESSING REQUIREMENTS:**

* Data Controllers must ensure:

1. Personal data shall be processed according to minimisation and won’t cause damage or distress to the data subject
2. Appropriate governance structures for the carrying out of the health research are in place, including -

(i) REC approval

(ii) Specification of the controller involved

(iii) Specify joint controllers

(iv) Specify any data processors

(v) Specify any person who is providing funding or otherwise supporting the project

(vi) Specify any person with whom it is intended to share any of the personal data collected and the purpose of such sharing

(vii) Provide training in data protection law and practice to those carrying out the health

research.

1. the following processes and procedures relating to the management and conduct of the health research must be in place:

(i) carrying out of an assessment of the data protection implications of the health research

(ii) where the assessment indicates a high risk to the rights and freedoms of individuals, the carrying out of a data protection impact assessment

(iii) demonstrate compliance with the data minimisation principle;

(iv) controls to limit access to the personal data undergoing processing in order to prevent unauthorised consultation, alteration, disclosure or erasure of personal data;

(v) controls to log whether and by whom personal data have been consulted, altered, disclosed or erased;

(vi) measures to protect the security of the personal data concerned

(vii) arrangements to anonymise, archive or destroy personal data once the health research has been completed;

(viii) other technical and organisational measures designed to ensure that processing is carried out in accordance with the Data Protection Regulation, together with processes for testing and evaluating the effectiveness of such measures.

1. arrangements to ensure that personal data are processed in a transparent manner are identified and in place;
2. **EXPLICIT CONSENT** has been obtained from the data subject, prior to the commencement of the health research, for the processing of his or her personal data for the purpose of specified health research, either in relation to a particular area or more generally in that area or a related area of health research, or part thereof.

**CONSENT:**

* **GDPR compliant consent must be:**

- freely given,

- specific,

- informed

&

- an unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

* Consent must be:

-Unbundled

-Active opt-in

-Specific

-Named

-Documented

-Easy to withdraw

-Freely given

-No blanket or opt-out consent permitted

* BROAD CONSENT
* The Health Research Regulation allows for specific broad consent in line with Article 7 and Recital 33.
* Provides that explicit consent from the individual must be obtained "for the purpose of the specified health research, either in relation to a particular area **or more generally in that area or a related area of health research,** **or part thereof**".
* This allows an individual to give his/her explicit consent where the research area is only generally defined and/or to give his/her consent only to certain areas of research or to parts of a particular research project.
* **At all times, the individual must be provided with sufficiently clear information to allow his/ her explicit consent to be informed and to represent the unambiguous indication of his/ her wishes**
* For example:
* Try to the greatest extent possible to describe future uses;
* Provide information on governance and objectives of the biobank;
* Purpose and aim of biobank;
* Funding & conflict of interest;
* Why the participant is being invited?
* Statement the participation is voluntary;
* Who has approved the research, risks & benefits of taking part;
* Type of data;
* What the biospecimens/data will be used for (any controversial areas?);
* Secondary processing;
  + Will the biospecimen/data be identifiable?
  + Rights/ ownership of samples;
  + Will biospecimens/data be shared;
  + Will they be shared with commercial entities;
  + Change of mind;
  + Dealing with deceased or incapacitated participants samples.
* Link to the Department of Health **‘Guidance on Information Principles for informed consent for the processing of personal data for health research’**:

<https://www.hrb.ie/fileadmin/1._Non-plugin_related_files/RSF_files/GDPR_guidance_for_researchers/Health_Research_Information_Principles.pdf>

* HRCDC-CLARIFICATION: The above document:” *is not a legally binding document, nor is it intended to be a complete and mandatory list of principles that must be addressed in patient information leaflet for the purposes of obtained consent.”*
* Three key points are set out in the document;

1. The onus is on the health researcher to (a) justify what information is or is not provided and (b) ensure that the data subject is not surprised by any use or disclosure of his or her personal health data by the researcher.
2. The researcher must always ensure that the language used avoids jargon and is easy to comprehend.
3. The information provided should be written from the perspective of the data subject and not the researcher. See the [WP29 guidance on transparency](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227)

* CAPACITY & CONSENT:
* Repeal of old Data Protection Act **removed** authority from list of “next-of–kin” to consent to research in absence of capacity.
* Has not been replaced.
* Only those with formal legal authority can now consent- power-of-attorney or ward
* DOH currently drafting guidelines in line with Assisted Decision-Making Act 2015:
* Presumption of capacity;
* Adequate trigger to question capacity?
* Duty to maximise capacity
* Functional test
* Categories of supported decision makers
* Will and preference as opposed to best interest.
* Problem areas =

1. Emergency medicine research;
2. Research in disability services.

* Currently following HSE Consent Policy in absence of guidelines and legislation.
* Risk/benefit analysis on case by case basis.
* Minors to be re-consented once reach adulthood.
* CONSENT DECLARATION COMMITTEE:
* May apply to the Consent Declaration Committee if Researcher of the view:
* the public interest in carrying out the research **SIGNIFICANTLY** outweighs the public interest in requiring the explicit consent of the data subject.
* statement setting out the reasons why it is not proposed to seek the consent of the data subject for the purposes of the health research.
  + <https://hrcdc.ie/making-an-application/>
* No more consent waivers through REC.
* The Committee has the power to:
* make a consent declaration
* make a consent declaration subject to conditions
* refuse to make a consent declaration
* revoke a consent declaration.
* The Committee may seek addition information to be provided within 15 days or the application will be refused.
* Must accept the Consent Declaration in writing within 30 days of notification - if not it will lapse.
* The Committee has the right to revoke a Declaration- you will be notified in writing of any intention to do so.
* There is a right to appeal decisions of the Committee.
* Must notify the Minister for Health and the Health Research Consent Declaration Committee of intention to appeal within **30 working days** from the date of notification of the decision by the committee.
* The appeal will be decided by an independent appeals panel appointed by the Minister for Health.
* No member of the Health Research Consent Declaration Committee will sit on an appeals panel.
* Committee not there as an alternative to seeking consent.
* What are the steps that need to be considered before applying for a Consent Declaration?
  + Consult the HRB’s GDPR guidance for researchers.
  + Consult the HRB’s consent declaration decision tree.
  + Determine whether your research project is a new project or if it is current.
  + Undertake a data protection impact assessment.
  + Ensure you have research ethics approval.
  + Consider whether or not the personal data can be anonymised.
  + For current research, determine if you have consent and whether or not the consent meets the standard of the previous Data Protection Directive 95/46/EC.
  + If yes, make reasonable efforts to contact the data subject who previously provided consent for the health research for the purposes of reobtaining consent from that data subject.
  + If not, consider if the data can be anonymised. Alternatively, consider if you can make a case that the public interest in continuing to carry out the health research significantly outweighs the public interest in requiring the explicit consent of the data subject together with a statement setting out the reasons why it is not proposed to seek the consent of the data subject for the purposes of the health research.
  + For new research, consider if you can make a case that the public interest in carrying out the health research significantly outweighs the public interest in requiring the explicit consent of the data subject together with a statement setting out the reasons why it is not proposed to seek the consent of the data subject for the purposes of the health research
* **DATA PROTECTION IMPACT ASSESSMENT:**
* A DPIA is required if ***at least two of these 10*** criteria are reached:

1. Evaluation or scoring- especially to do with someone's work performance or health e.g. a biotechnology firm offering genetic testing to customers in order to predict disease/health risks;
2. Automated-decision making with legal or similar effect - the processing may lead to discrimination or exclusion;
3. Systematic monitoring - e.g. cctv in a public space;
4. **Sensitive Data- e.g. health data, genetic data and all article 9 special categories of data**
5. Data Processing on a large scale;
6. Datasets that have been matched or combined;
7. **Data concerning vulnerable data subjects -power imbalance between data controller and data subject e.g. patients, children, the elderly, employees, persons with disabilities**
8. Innovative use or applying technological or organisational solutions - e.g. fingerprint or facial recognition;
9. Data transfer outside the EU;
10. Where the processing itself prevents a data subject from accessing a service- e.g. credit screening by banks to decide whether to give someone a loan.

* In terms of health research, criteria 4 & 7 nearly always apply, and sometimes 1, 5 &9 also.
* **Components of a DPIA:**

1. A systematic description of the processing is provided; (data mapping schedule useful here)

* Nature, scope, context and purposes of the processing are taken into account
* Personal data, recipients and period for which the personal data will be stored are recorded;
* A functional description of the processing operation is provided;
* The assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified
  + Compliance with approved codes of conduct is taken into account

1. Necessity and proportionality are assessed;
   * + - specified, explicit and legitimate purpose(s);
       - lawfulness of processing;
       - adequate, relevant and limited to what is necessary data;
       - limited storage duration;
       - information provided to the data subject ;
       - right of access and portability;
       - right to rectify, erase, object, restriction of processing;
       - recipients;
       - processor(s) ;
       - safeguards surrounding international transfer;
       - prior consultation
2. Risks to the rights and freedoms of data subjects are managed;

* Origin, nature, particularity and severity of the risks are appreciated or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
* risks sources are taken into account;
* potential impacts to the rights and freedoms of data subjects are identified in case of illegitimate access, undesired modification and disappearance of data;
* threats that could lead to illegitimate access, undesired modification and disappearance of data are identified;
* likelihood and severity are estimated;
* Measures envisaged to treat those risks are determined

1. Interested parties are involved

* The advice of the DPO is sought
* The views of data subjects or their representatives are sought
* SECURITY:
* Appropriate encryption is used - particularly for laptops, tablets, portable storage devices and cloud storage folders;
* Appropriate security is used on smartphones, for example, finger print recognition;
* Special categories of data is sent by encrypted email only;
* Password-protect access to devices employing the use of strong passwords and password managers;
* Work related devices are separated from those used for personal use; i.e. tablets, computers and other such devices;
* Work related devices are not used by any family members or other third party;
* Data is appropriately backed-up and any devices used for back-ups are appropriately secure;
* No personal data is contained on old devices when they are being retired;
* Documents are not saved or left open on open-access computers;
* Electronic files are destroyed in accordance with a data retention and destruction policy;
* All support staff receives appropriate training in relation to data protection and-communications policies are put in place for staff;
* Up-to-date anti-virus software and firewalls are used and operating system updates are applied;
* When making back-ups of data, using facilities which would not be at risk in the event of a ransomware attack
  + Compliance with the Legislation and Regulation is the responsibility of the Principle Investigator (PI) (who is also the Data Controller) and the Data Protection Officer.
  + It is important to note that the Clinical Research Ethics Committee’s only reviews applications from an ethical perspective.
  + Data Protection Legislation is the responsibility of the PI and DPO.

REFERENCES:

1. Mary Kirwan, Barrister-at-Law
2. Health Research Board:

* Information principles <https://www.hrb.ie/fileadmin/1._Non-plugin_related_files/RSF_files/GDPR_guidance_for_researchers/Health_Research_Information_Principles.pdf>
* HRB Guidance page: <https://hrcdc.ie/guidance/>

1. HSE Privacy Statement <https://www.hse.ie/eng/privacy-statement/>
2. Health Research Authority, NHS <https://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/>