PHILIPLEE

DATA PROTECTION IMPACT ASSESSMENTS & HEALTH RESEARCH
A BEGINNER'S GUIDE

Anne Bateman, CIPP/E

8 June 2022

Outline of today's workshop

- Overview of the DP rules which apply to health research
- What is a DPIA? What are its objectives in a health research context?
- When is a DPIA required for health research?
- DPIA logistics
- Walk through a DPIA in a research setting
- How to document and mitigate data protection risks in respect of health research
- Q&A

WHAT IS A DPIA?

OBJECTIVES IN A HEALTH RESEARCH CONTEXT

DPIA – a summary #1

- Documented risk assessment process, by reference to data protection rules (GDPR, national DP legislation and regulatory guidance)
- To assess and demonstrate compliance with data protection rules for certain projects / systems that are going to collect and use personal information of individuals
- Looks at risks to individuals from the collection and use of their personal information, at proposal stage, before any collection of personal information happens
- Assesses what measures to take to mitigate identified risks
- *"DPIA is a process for building and demonstrating compliance"* – WP29 Guidance on DPIAs (April 2017) (adopted by EDPB)
- If outcome of DPIA indicates difficult-to-mitigate risks, DPC consultation

DPIA – a summary #2

- Normally, A.35 GDPR sets out the triggers for when a DPIA is required, supplemented by EU and national guidance
- e.g. A.35 GDPR triggers for health research include:-
  - Proposals to "process" on a large scale sensitive categories of personal information such as health data, genetic data or biometric data; "large scale" not defined in the GDPR or in guidance
  - Proposals to engage in "processing" of personal information that would be likely to result in "high risk to the rights and freedoms of individuals"
- **BUT!** In Ireland, for "health research", the rules for DPIA triggers are more specifically set – by the Data Protection (Health Research) Regulations 2018 (amended in 2019 and 2021) (**DPHRR**)
- Under DPHRR, either need an "***assessment of data protection implications of the health research***" or (if high risks to individuals) a **DPIA**

DPIA – a summary #3

- "Health research" as defined by DPHRR:-

(i) research with the goal of understanding normal and abnormal functioning, at molecular, cellular, organ system and whole body levels
(ii) research that is specifically concerned with innovative strategies, devices, products or services for the diagnosis, treatment or prevention of human disease or injury
(iii) 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
(iv) research with the goal of improving the efficiency and effectiveness of health professionals and the health care system
(v) research with the goal of improving the health of the population as a whole or any part of the population through a better understanding of the ways in which social, cultural, environmental, occupational and economic factors determine health status

A QUICK LOOK AT THE HSE DPIA TEMPLATE

PHILIPLEE

DUBLIN | BRUSSELS | SAN FRANCISCO

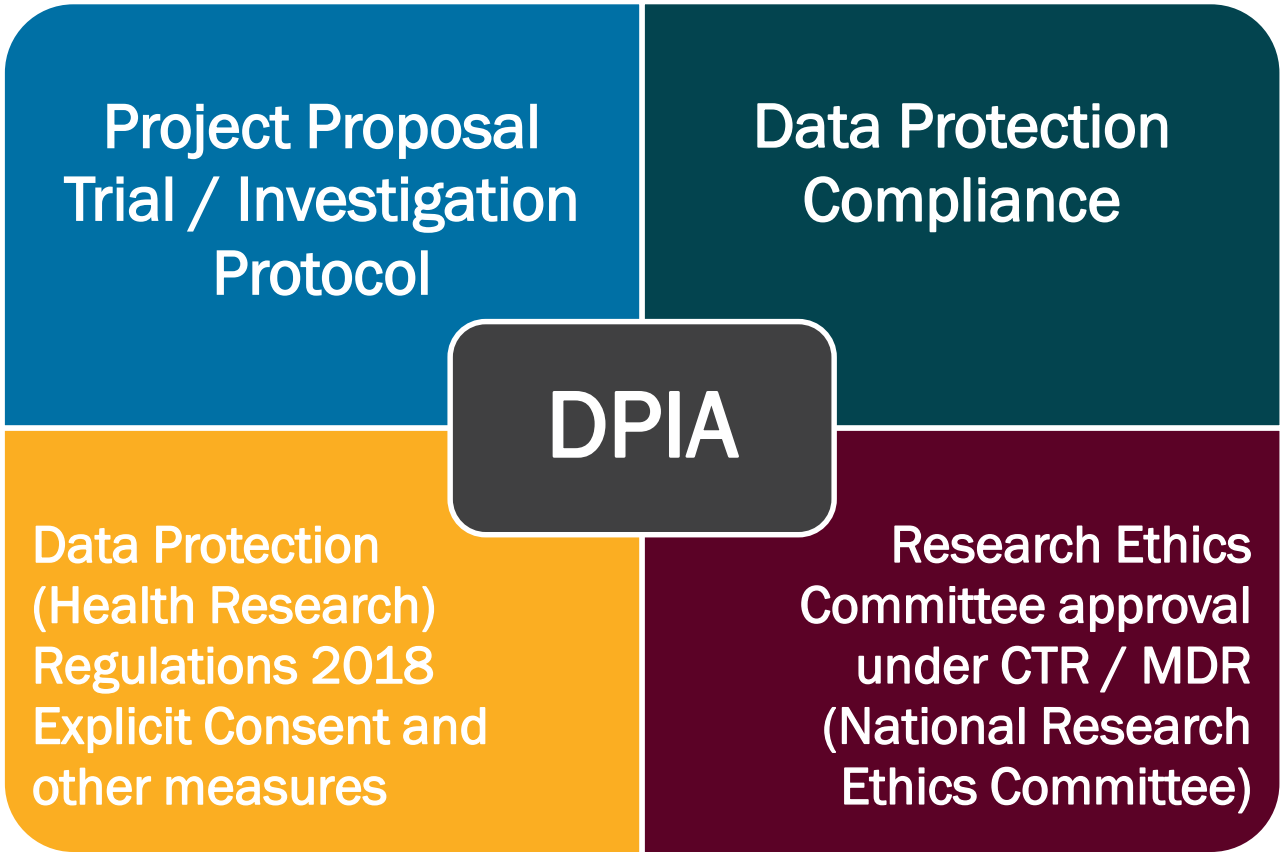
THE DPIA & HEALTH RESEARCH

SOME REGULATORY CONTEXT

PHILIPLEE

DUBLIN | BRUSSELS | SAN FRANCISCO

DPIAs in health research – context



DPIAs – health research examples

- **Example 1:** Proposal for a clinical trial on investigative medicinal product (regulated by the Clinical Trial Regulation 2014 (CTR)) or a proposal for a clinical investigation on a medical device (regulated by the Medical Devices Regulation 2017 (MDR)) – HSE/hospital as single site or part of a multi-site
- **Example 2:** Proposal to conduct health research on existing bank of patient records under control of the HSE/hospital, in collaboration with another public/private entity
- **Example 3:** Establishment of a disease registry or biobank, in control of HSE, to which other entities will be given access for the purposes of ongoing research

DPIAs – what to assess (HSE template)

- What **personal data** of **data subjects** is the project going to collect and use? (What **processing** of personal data is going to be undertaken?)
- What are the **purposes** of the project? Do these purposes conform with the **data protection rules**?
- What are the **legal bases/conditions under the GDPR** for the proposed processing? Influence of the DPHRR and its req'mt of explicit consent
- Who is the **data controller**? Why is this relevant?
- Are there **data processors** involved? How do we identify them?
- Will there be **data sharing**? What does this mean? Will there be **data transfers**? What does this meant? How do we deal with these?
- What **technical and organisational security measures** are expected?

OVERVIEW OF DATA PROTECTION

PHILIPLEE

DUBLIN | BRUSSELS | SAN FRANCISCO

Data Protection: what is it?

- Data Protection = set of rules governing how organisations collect and use personal information (*"personal data"* and *"special category data"*) of individuals (*"data subjects"*)
- Places legal obligations on the *"processing"* of personal data by *"data controllers"* and *"data processors"*
- Regulatory scrutiny (Data Protection Commission), possible fines and/or criminal penalties if the obligations are breached, +compensation to affected individuals, +reputational damage
- All public and private sector organisations *"process"* personal information as fundamental part of normal business and operations
- Paper- and electronically-held information

Legal Sources

- Main rules contained in the **EU General Data Protection Regulation (GDPR)** (enacted May 2016, came into legal effect on 25 May 2018)
- Supplemented by the **Data Protection Acts 1988 – 2018** and (for health research) the **Data Protection (Health Research) Regulations 2018 – 2021** (**DPHRR**)
- **NB** Fundamental basis in human rights: **right to privacy** and **right to protection of personal data**, Articles 7 and 8 EU Charter of Fundamental Rights

Who enforces? Who provides guidance?

- National Data Protection Supervisory Authorities (**DPSAs**) appointed under GDPR and national implementing legislation
- Ireland = Data Protection Commission, www.dataprotection.ie
- DPSAs provide national guidance on GDPR rules
- European Data Protection Supervisor (**EDPS**): monitors and supervises EU institutions' DP compliance, under EU Regulation 2018/1725
- European Data Protection Board (**EDPB**), collective group of national DPSAs + EDPS
- EDPB guidance is important, https://edpb.europa.eu/edpb_en
- + Health Research Board (www.hrb.ie) +HRCDC

Personal Data in health research

- **Personal Data:** any information relating to an identified or identifiable natural person; in particular by ref to an identifier such as a name, ID number, location data, online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person
- E.g. Patient name, address, age, DOB, PPSN, contact details, financial information
- **Special Category Data:** specific types of personal data listed in the GDPR that are considered especially sensitive, including **data concerning health** (includ. related to provision of health care services and data revealing health status), **genetic data**, **data revealing racial or ethnic origin**, **biometric data**, **data concerning sex life**

Processing in health research

- **Processing**: any operation of set of operations which is performed on personal data (or on sets of personal data), manual or automated, e.g. collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, **consultation**, **use**, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

- In health research, e.g.:-
  - Accessing and consulting existing records of patient data
  - Identifying and gathering information on specific patients for recruitment
  - Records of contact with and responses from potential patients
  - Setting up and holding database of study/research participants
  - Amending patient information in your data set
  - Sharing patient information internally and externally
  - Anonymising or pseudonymising the data set
  - Archiving or deleting the data set

Who is regulated? Who is responsible? Controllers and Processors #1

- Concepts of data controller and data processor
- Data controller is responsible for GDPR compliance, including for conducting DPIAs
- "Controller" (**A4.7 GDPR**): *person…which alone or jointly with others determines the purposes and means of the processing of personal data*
- "Processor" (**A4.7 GDPR**): *person, public authority, agency or other body which processes personal data on behalf of the controller*; separate entity to the data controller
- Key determinant = independent control over personal data; decides on the key elements of the processing; issue of fact

Who is regulated? Who is responsible? Controllers and Processors #2

- Data controllers decide on the ***why*** and the ***how*** of the processing
- EDPB Guidance says that the data controller determines purposes and "essential means" such as (in the context of health research):-
  - **The purpose of the research**: Who initiates the research? Who drafts and determines the contents of the study proposal / protocol?
  - **The types of personal data will be processed**: What are the characteristics of the patient group? What personal data is needed in order to conduct the research?
  - **The duration of the processing**: How long will the research last? How long (subject to legal requirements) will the patient data be stored for?
  - **Access to the personal data**: Who contracts with the research site(s)? Who has legal control over data storage and access?

Who is regulated? Who is responsible? Controllers and Processors #3

- GDPR provides for the concept of **joint controllers**: two or more controllers which jointly determine the purposes and means of processing
- Possibilities in the context of health research, fact-dependent:-
  - **Sponsor** of the clinical study/clinical trial/clinical investigation: initiate the research (but for them, no research); draft/approve the protocol; legal responsibility HPRA authorisations, pharmacovigilance and site files
  - **Principal Investigator**: may initiate the research (alone or with sponsor); may be involved in protocol; independent medical professional with responsibility for patient care and confidentiality
  - **Site (HSE/voluntary hospital)**: if making decisions on purposes, essential means, e.g. research on existing patient data set; biobank

Who is regulated? Who is responsible? Controllers and Processors #4

- Specific example of **joint control in research** from EDPB Guidance**:**
  - *"Research project by institutes: Several research institutes decide to participate in a specific joint research project and to use to that end the existing platform of one of the institutes involved in the project. Each institute feeds personal data it already holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes however is a separate controller for any other processing that may be carried out outside the platform for their respective purposes."*

Who is regulated? Who is responsible? Controllers and Processors #5

- Specific example on **clinical trial** from EDPB Guidance**:**
  - *"A healthcare provider (the investigator) and a university (the sponsor) decide to launch together a clinical trial with the same purpose. They collaborate together to the drafting of the study protocol (i.e. purpose, methodology/design of the study, data to be collected, subject exclusion/inclusion criteria, database reuse (where relevant) etc.). They may be considered as joint controllers, for this clinical trial as they jointly determine and agree on the same purpose and the essential means of the processing. The collection of personal data from the medical record of the patient for the purpose of research is to be distinguished from the storage and use of the same data for the purpose of patient care, for which the healthcare provider remains the controller. In the event that the investigator does not participate to the drafting of the protocol (he just accepts the protocol already elaborated by the sponsor), and the protocol is only designed by the sponsor, the investigator should be considered as a processor and the sponsor as the controller for this clinical trial."*

Who is regulated? Who is responsible? Controllers and Processors #6

- Further example on **health data analysis** from EDPB Guidance**:**
  - *"Company ABC, the developer of a blood pressure monitoring app and Company XYZ, a provider of apps for medical professionals, both wish to examine how blood pressure changes can help predict certain diseases. The companies decide to set up a joint project and reach out to Hospital DEF to become involved as well. The personal data that will be processed in this project consists of personal data which Company ABC, Hospital DEF and Company XYZ are separately processing as individual controllers. The decision to process this data to assess blood pressure changes is taken jointly by the three actors. Company ABC, Hospital DEF and Company XYZ have jointly determined the purposes of processing. Company XYZ takes the initiative to propose the essential means of processing. Both Company ABC and the Hospital DEF accept these essential means after they as well were involved in developing some of the features of the app so that the results can be sufficiently used by them. The three organizations thus agree on having a common purpose for the processing which is the assessment of how blood pressure changes can help predict certain diseases…."*

Who is regulated? Who is responsible? Controllers and Processors #7

- Further example on health data analysis from EDPB Guidance, continued:
  - *"….. Once the research is completed, Company ABC, Hospital DEF and Company XYZ may benefit from the assessment by using its results in their own activities. For all these reasons, they qualify as joint controllers for this specific joint processing.*

If Company XYZ had been simply asked by the others to perform this assessment without having any purpose of their own and merely been processing data on behalf of the others, Company XYZ would qualify as a processor even if it was entrusted with the determination of the non-essential means."

Who is regulated? Who is responsible? Controllers and Processors #8

- Data processors do not determine purposes and essential means
- EDPB says that they can determine "non-essential means", e.g.
  - **Site (HSE/voluntary hospital):** can provide use of patient appointment system and e.g. data storage under contract with Sponsor/Investigator, even if HSE/hospital has already licensed the IT system/database, set the security parameters on the IT system/database
  - **Principal Investigator:** if merely following the instructions of the Sponsor and no involvement in the protocol (per EDPB Guidance)
  - **Contract Research Organisation (CRO):** contracted by Sponsor/Investigator to assess with all logistics and administration for trial, but no independent decision-making on purposes and means of the personal data processing

Who is regulated? Who is responsible? Controllers and Processors #9

- Common data processor arrangements for health research:-
  - Contract Research Organisations (as before)
  - Third party IT suppliers (including database suppliers), with access to the patient database for support and maintenance purposes
  - Cloud storage providers/hosting services

QUERY FOR DISCUSSION

HOW DO YOU SPECIFY YOUR ORGANSATION? DATA CONTROLLER OR JOINT CONTROLLER OR DATA PROCESSOR?

OVERVIEW OF DATA PROTECTION RULES + APPLICATION TO HEALTH RESEARCH & DPIAS

PHILIPLEE

DUBLIN | BRUSSELS | SAN FRANCISCO

Relevant GDPR Rules #1 Legal Basis

1. Have a **legal basis for processing of personal information**
   - Available legal bases for "regular" personal data are set out in A.6 GDPR
   - Additional condition for "special category data" set out in A.9 GDPR (plus need to point to an underlying A.6 basis)

- In health research, most suitable, usual A.6 GDPR legal bases are:-
  - **Consent** of the patients / research subjects (A.6(1)(a))
  - **Necessary for fulfilling legal obligation** (A.6(1)(c)) (e.g. under CTR, MDR, pharmacovigilance)
  - **Necessary for task in the public interest** or **exercise of official authority** (A.6(1)(e)) – public interest task also available to private entities
  - **Legitimate interests** (A.6(1)(f)), but not applicable to processing carried out by public bodies in the performance of their tasks; common for sponsors, investigators and sites in the private sector

Relevant GDPR Rules #1 Legal Basis

- In health research, most suitable, usual A.9 GDPR conditions for the processing of special category data are:-
  - **Explicit consent** of the patients / research subjects (A.9(2)(a))
  - **Processing necessary for public interest in the area of public health** (A.9(2)(i)), including ensuring high standards of quality and safety of health care and of medicinal products and medical devices; provision of "**suitable and specific measures**" to safeguard individuals' rights, including professional secrecy
  - **Processing necessary for scientific or historical research** (A.9(2)(j) + **A.89(1)**), proportionate, measured and subject to "**suitable and specific measures**" to safeguard individuals' rights

(A.89(1) requires processing for scientific research purposes to be subject to appropriate safeguards to ensure technical and organisational measures res taken to implement (in particular) data minimisation; e.g. pseudonym'tn)

Relevant GDPR Rules #1 Legal Basis

- GDPR also allows Member States to keep/introduce further conditions and limitations for the processing of health data, genetic data and biometric data
- Ireland has done this, via the Data Protection Act 2018 and the DPHRR, and these additional conditions affect what A.6 legal basis and what A.9 conditions a data controller engaging in health research can use
- **Upshot is that the DPHRR in effect require that "consent" / "explicit consent" is used as the legal basis for health research, irrespective of the other legal bases available under the GDPR itself** (except for preliminary assessments of eligibility for health research)
- If can't get explicit consent, must make application for consent declaration to the HRCDC under the DPHRR (high standard)

Relevant GDPR Rules #1 Consent issues

- Difference between informed patient consent (medical, ethical requirement; CTR, MDR requirements) **–v-** consent as legal basis to process personal data
- May have to (and be able to) obtain informed patient consent, **BUT** consent/explicit consent may **not** be the most appropriate legal basis under the GDPR
- Must decide whether can fulfil rules for valid consent under GDPR
- GDPR consent: *"means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he/she, by a statement or clear affirmative action, signifies agreement to the processing of personal data relating to him/her"*
- Consent can be withdrawn at any time

Relevant GDPR Rules #1 Consent issues

- Main practical issues for consent-based processing under GDPR:-
  - Imbalance of power (casts doubts over whether consent is freely given); EDPB: *"implies real choice and control for data subjects"*; no clear imbalance between individual and data controller
  - Can't be fully specific about purposes and processing activities
  - Withdrawal of consent would cause issues for the research, or can't fully action withdrawal
  - Using historic data and can't clearly demonstrate consent to required level under GDPR
  - Previous consent obtained did not meet the high standards required under the GDPR (e.g. telling someone about their right to withdraw consent)
  - Purposes, activities have evolved beyond the original consent (secondary uses of patient data)

Relevant GDPR Rules #1 Clinical Trials, EDPB

- EDPB Opinion 3/2019 on interplay between GDPR and CTR (appropriate legal basis for CTs and what are primary and secondary uses)
- EDPB Document on 2 February 2021 on consistent application of GDPR in relation to health research
- For clinical trials, EDPB says:-
  - Primary use of clinical trial data = all processing operations related to a specific clinical trial protocol during whole lifecycle of clinical trial
  - Within primary use, will be different purposes, with different legal bases
  - Main two purposes: **(1)** research activities (legal basis = A6(1)(a)+A9(2)(a) or A6(1)(e)/A6(1)(f)+A9(2)(i)/A9(2)(j)); and **(2)** protection of health processing, e.g. safety reporting, archiving CT master file and medical files, regulatory inspections (legal basis = A6(1)(c)+A9(2)(i))

Relevant GDPR Rules #1 Clinical Trials, EDPB

- For clinical trials governed by the CTR, EDPB also says:-
  - If consent = legal basis, remember that individual is allowed to withdraw their consent at any time
  - Data processing conducted up to time of withdrawal is lawful; however, data controller must then stop processing and delete personal data unless has another legal basis for continuation of processing, e.g. legal obligation for safety reporting
  - Whether secondary use of personal data is permitted for health research purposes without new legal basis depends on context: A.5(1)(b) GDPR permits processing for "compatible purposes"; potentially okay if processing is conducted in conformity with A.89 GDPR

QUERY FOR DISCUSSION

WHAT LEGAL BASES / CONDITIONS ARE RESEARCHERS RELYING ON CURRENTLY?

Relevant GDPR Rules #2

2. Lawfulness, fairness and transparency: processing must be lawful (e.g. not breach patient confidentiality), fair, and **transparent**

   - Transparency usually through **Privacy Notice** but for health research, can be done through patient information leaflet / informed patient consent form / explicit consent form, usually via treating HCP
   - Note that A.13 GDPR and A.14 GDPR set out specific transparency information that must be given to individuals, but are exceptions (e.g. for indirectly-obtained data, transparency is impossible or would involve disproportionate effort)
   - DRHRR also require transparency as a S&SM

Relevant GDPR Rules #3

3. **Purpose limitation**: collect personal information only for **identified, specific & lawful purposes** + **processing must be compatible** with these purposes

   - Note that A.5(1)(b) GDPR (which sets out this requirement) sets out a presumption of compatibility where further processing is conducted on personal data for e.g. scientific research purposes, i.e. secondary uses

   - However if *de facto* Irish legal basis is consent/explicit consent, will be difficult for researchers to rely on this exception under A.5(1)(b)

Relevant GDPR Rules #4, #5

4. **Data minimisation**: personal information processed must be **adequate, relevant & limited to what is necessary**, linked to the purpose for which collected – GDPR and DPHRR both have a particular focus on this **data minimisation** concept
   - Will the quality of the patient data be good enough for the research project's purposes?
   - Which patient data could you not use, without compromising the needs of the project?
5. **Data accuracy, data quality**: Ensure personal information is **accurate** and, where necessary, **kept up-to-date**

Relevant GDPR Rules #6

6. **Storage limitation, data retention**: Keep personal information in a form that permits identification for no longer than necessary (related to the original purpose for which it was collected), i.e. be able to specify retention periods for the personal data

   - Some retention periods are specified by legislation, e.g. for clinical trials governed by the CTR, site master file must be archived for 25 years; medical files for periods specified under national law

   - A.5(1)(e) GDPR recognises necessity to retain personal information related to health research for longer periods, as long as appropriate safeguards are put in place and technical and organisational measures

Relevant GDPR Rules #7

7. **Data security, integrity and confidentiality**: Ensure appropriate security of the personal information; protect against (internal or external) unauthorised or unlawful processing, and against accidental loss, destruction or damage, using appropriate technical and organisational measures

   - Taking into account state of the art, risks for personal information, controller and processor must implement appropriate technical and organisational measures, including:-
     - Pseudonymisation and encryption of personal information
     - Ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems
     - Ability to restore availability and access to personal information quickly in event of physical or technical incident
     - Processes for regular testing, assessing, evaluation effectiveness of security measures taken

Relevant GDPR Rules #8

8. **Accountability**: data controller must be able to demonstrate compliance with the data protection principles and with its data protection obligations in general + obligation to implement appropriate technical and organisational measures to ensure and be able to demonstrate that its data processing is GDPR-compliant

   - DPIA is a process that enables a data controller to (a) meet its accountability obligation, and (b) assess whether it is meeting its compliance obligations generally ref specific projects such as health research

Relevant GDPR Rules #9

9. **Individuals have rights**, including right to access their personal information on request + data controller must explain these rights in order to comply with transparency requirements, e.g.
   - **Right of access to personal data**, on request, usually within one month + accompanying transparency information obligation
   - **Right to rectification of inaccurate data**: can be correction, completion or supplementary statement
   - **Right to erasure**, e.g. if purpose of processing no longer applies, if withdraw consent, or if processing unlawful, but exception if processing is necessary for scientific research purposes, subject to safeguards and deletion of the personal information is likely to seriously impair the objectives of the research

Relevant GDPR Rules #10, #11

10. **Vet data processors** (especially robustness of their security) and have **written agreements with them**

11. **No transfers of personal information outside the European Economic Area** (EEA) unless certain transfer mechanisms are in place
    - Available transfer mechanisms are specified in Chapter V GDPR (A.44 – A.50 GDPR)
    - For DPIA, need to identify whether any personal data (identifiable information) will transfer out of the EEA, e.g. to sponsor based outside the EEA: need technical and legal guidance if it is proposed to transfer data outside EEA

CONDUCTING A DPIA
HOW TO PRACTICALLY APPROACH

PHILIPLEE

DUBLIN | BRUSSELS | SAN FRANCISCO

Conducting a DPIA #1

- Assumption that you have determined that your organisation is the data controller or is a joint data controller and it is appropriate to take responsibility for conducting the DPIA
- Document the proposed project from perspective of data processing activities
- Activity Details:
  - Summary of research project proposal or protocol with description of data processing activities involved; attach the project proposal or protocol
  - Explain broadly what the project aims to achieve: this helps with showing necessity for the processing and with underpinning the legal basis (if other than explicit consent) + shows intended effects on individuals
  - Outline the proposed size of the patient group, including control groups

Conducting a DPIA #2

- Activity Details: Explain what types of data processing are going to be involved, taking each data processing step in sequence; use data flows and diagrams if useful:-
  - Data collection: How identify potentially eligible patients? Data sources? Consultation with existing files? How collect and verify their information? What data will be collected at assessment stage?
  - Data collation, use: What will you do with patients' information once they are recruited? What information will you collect and store? How often? How will you use that information? How will you comply with your data minimisation, data accuracy and data quality obligations?
  - Data storage: How will the information be stored? What TOMs will be applied to meet your data security obligations? Pseudonymisation? Encryption? Describe also how security techniques align with trial/research requirements (e.g. if trial is to be randomised, double-blind)

Conducting a DPIA #3

- Data sharing: Who will you be sharing data with and why? What contractual or other arrangements are in place with those persons/entities? What status do they have? E.g. are they data processors?
- Data archiving, deletion: What data needs to be retained in live/readily accessible format? What data can/needs to be archived? What data can be deleted/deidentified/anonymised and when?

Conducting a DPIA #4

- Identify legal basis (as discussed)
- Identify data controller or joint controllers (as discussed)
- Identify data processors and their activities (as discussed), outline contractual arrangements and security applied by processors
- Automated decision-making: unlikely for health research
- Explanation of necessity of all personal data being collected: explain in context of purposes for research, why necessary to examine those data points; explain also in context of legal obligations (e.g. safety, pharmacovigilance); explain how you meet obligations of data quality, data accuracy and data minimisation
- How are data subjects informed of the processing? Usually through treating HCP, with patient information leaflet – confirm and describe this

Conducting a DPIA #5

- Identification of risks, e.g. unauthorised access to data, unauthorised modification of data, accidental or intentional deletion of data
- Provide realistic examples of how they might occur, e.g. laptops, devices containing datasets are stolen or lost; accidental email to someone other than trial subject
- Risks to individuals, e.g. sensitive personal data relating to health – could cause damage/distress if access, shared or lost
- Ref. risks to individuals, may be necessary to asses whether certain personal data is already made public by the individuals, e.g. through patient advocacy, public social media accounts

Conducting a DPIA #6

- Describe options to reduce or mitigate the identified risks, e.g.
  - Use of organisation-only encrypted laptops, devices and folders, files; datasets stored on secure servers, with restricted access to project folders
  - No patient identifiers in datasets (pseudonymisation techniques, e.g randomised numbers for patients, keys not kept on same site)
  - Documented internal policies and procedures, e.g. what data to give out over phone, verification of individuals who make enquiries, only disclosures through HCP
  - Verification of data collection forms ref excessive or unnecessary personal data; limited ability for patients to supply unnecessary or excessive personal data
  - Policies around sending of datasets via email or other communications; strong password protections for shared datasets; no emails; use of data rooms
  - No personal devices; no communication through personal emails, DMs
  - Periodic review of pseudonymised datasets to assess whether can be fully deidentified

Conducting a DPIA #6

- Consider TOMs/S&SMs that must be applied under DPHRR and integrate these into DPIA (and some of these are GDPR obligations anyway, so not sufficiently specific and circular)
  - Access limitations within organisation (data security obligation)
  - Strict time limits for erasure (data retention obligation)
  - Training for researchers and project administrators
  - Logging mechanisms to permit verification
  - Designation of a DPO (GDPR obligation for public bodies)
  - Processing undertaken under supervision of medical professional
  - Pseudonymisation and encryption (data security obligation)
  - Ethics committee approval (DPHRR)

Conducting a DPIA #7

- Takes time + need to build in time for data subject consultation, processor/service provider engagement and DPC consultation, if required
- Multi-disciplinary input, including from IT
- DPO doesn't conduct it, but advises on it (catered for in standard template)
- Continuously reviewed and regularly re-assessed
- Not necessary to publish, but seen as good practice in transparency
- The case for drafting standard responses to the template DPIA across the organisation, e.g. ref relevant TOMs, standard mitigation measures, etc.

Q&A / Thank you

PHILIPLEE

philiplee.ie
info@philiplee.ie

DUBLIN
7/8 Wilton Terrace
Dublin 2
Ireland
T: +353 (0)1 237 3700
F: +353 (0)1 678 7794

LONDON
2 Eastbourne Terrace
London, W2 6LG
United Kingdom
T: +44 (0)20 3934 7010
F: +353 (0)1 678 7794

BRUSSELS
39 Rue des Deux Eglises
1000 Brussels,
Belgium
T: +353 (0)1 237 3700
F: +353 (0)1 678 7794

SAN FRANCISCO
201 Spear Street, Suite
1100 CA 94105,
United States
T: +353 (0)1 237 3700
F: +353 (0)1 678 7794