

Data Privacy Impact Assessment (DPIA)

A data privacy impact assessment (DPIA) is a process to identify and address privacy issues associated with a Research study/Clinical Trial that involves processing of personal data.

**STAGE 1: Threshold assessment- is a DPIA required?**

Article 35 of the GDPR requires the Hospital to conduct a DPIA if a study could potentially cause privacy issues. You need to conduct a DPIA if your study involves any of the following:

**5 STAGES of the PIA PROCESS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Transfer of data outside the EU |  |  | Outsourcing of patient samples to third parties for analysis | Y | N |
| Processing of vulnerable person’s data or children’s data |  |  | Processing of genetic/ biometric data |  |  |
| Data shared with or accessed by 3rd parties |  |  | Use of identifiable data for secondary purposes e.g. Clinical audit |  |  |
| Personal data used to evaluate performance |  |  | Any other reasons that may affect privacy |  |  |
| Data Processing on a large scale |  |  |  |  |  |
| Processing of large volumes of special category data\* |  |  | If you are unsure if a DPIA is required contact ResearchEthics@tuh.ie |  |  |

**\***Special category data: This data is more sensitive, and so needs more protection. For example, information about an individual’s race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life; or sexual orientation.

**If your project requires a DPIA proceed to stage 2**

|  |  |
| --- | --- |
| **Study Title** |  |
| **Study Owner** |  |
| **Author of this DPIA**  **Contact Details** |  |
| **Department** |  |
| **Directorate** |  |
| **Date** |  |
| **STAGE 2: Identify Privacy Risks** | |
| **Describe the Clinical Trial/Research Study, include aims and objectives, and benefits of the Study. Describe what type of processing it involves**. **Is this study being conducted on a rare condition or on a condition that could lead to the identification of a participant (Max 350 words)** | |
|  | |
| **What is the purpose of collecting the data for this study?** | |
|  | |

|  |  |  |
| --- | --- | --- |
|  | **What Personal Data will be Collected?** | |
| **Information that identifies the individual and their personal characteristics** | Name | ☐ |
| Address | ☐ |
| Postcode | ☐ |
| Dob | ☐ |
| Age | ☐ |
| Sex | ☐ |
| Gender | ☐ |
| Racial/ethnic origin | ☐ |
| Tel no. | ☐ |
| Physical description | ☐ |
| PSS Number |  |
| Mobile/home phone no. | ☐ |
| Email address | ☐ |

**What Sensitive Personal Data will be collected?**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Yes** | **N/A** |
|  | Information relating to the individual’s physical or mental health or condition.  Information relating to genetic information(biological samples such as chromosomal or DNA samples) and biometric information( such as fingerprints or facial recognition) | ☐ | ☐ |
|  | Is the Research Study/Clinical Trial being conducted on a rare condition ? | ☐ | ☐ |
|  | Does the research involve a recorded interview or photographs that could identify the participant? | ☐ | ☐ |
|  | Information relating to the individual’s sex life. | ☐ | ☐ |
|  | Information relating to the individual’s sexual orientation | ☐ | ☐ |
|  | Information relating to the family of the individual and the individuals lifestyle and social circumstances | ☐ | ☐ |
|  | Information relating to any offences committed or alleged to be committed by the individual | ☐ | ☐ |
|  | Information relating to criminal proceedings, outcomes and sentences regarding the individual | ☐ | ☐ |
|  | Information which relates to the education and any professional training of the individual | ☐ | ☐ |
|  | Employment and career history | ☐ | ☐ |
|  | Information relating to the financial affairs of the individual | ☐ | ☐ |
| Information relating to the individual’s religion or  other beliefs | | ☐ | ☐ |
| Information relating to the individual’s membership of a trade union. | | ☐ | ☐ |

**What is the lawful Basis for Collecting this Information?**

**Tick**

|  |  |
| --- | --- |
| Explicit Consent |  |
| Legitimate interests of the Hospital (Controller of Medical Records) |  |
| Legitimate interests of the Study Sponsor(Controller of Study Data) |  |
| Vital Interests of the data subject or another person |  |
| Carried out (internally) by a not-for-profit organisation |  |
| Information that has been already made public by data subject |  |
| Necessary for substantial public interest |  |
| Necessary for reasons of public interest in the area of public health |  |
| Archiving purposes in the public interest/ Scientific or Historical Research purposes/ Statistical purposes |  |

**How Will You Keep This Data Secure?**

**TICK /ADD COMMENTS/PROVIDE DETAILS**

|  |  |
| --- | --- |
| Will the information be  1) Anonymised (please note that where possible information should be anonymised) |  |
| 2) Pseudonymised  (If data is pseudonymised (coded) who will hold the key?) |  |
| 3) Identifiable |  |
| Where are you obtaining the data from?  e.g. Healthcare records, Staff, Patient |  |
| Where will the information be stored and how will you keep it safe?  E.g. locked cabinet, excel, limited access, encryption, strong passwords.  In what form will the information be stored (Anonymised, Pseudonymised or Identifable) |  |
| Who will have access to the data? |  |
| How long will the data be stored? |  |
| Will data be stored off site? |  |
| Will data be shared with third parties including ICT cloud providers, cloud services, sub-contractors?  What cloud server is being used?  Where is the server located? |  |
| Will any personal or sensitive data be transferred to a country outside of the EU?  What country is data transferred to?  What data will be transferred?  How is the data transferred? |  |
| If you are transferring data outside the EU what  Security measures/ appropriate safeguards are in place?  Provide details:  Adequacy decision/ US privacy shield/  Standard contractual clauses/ legally binding contract/  Authorisation from Data Protection Commissioner |  |
| How long will you retain the data & why? |  |
| How will you destroy the data after it is no  Longer required?  Who will destroy the data after it is no longer required? |  |
| Have you collected only essential data that is  necessary for the project (data minimisation) |  |
| What arrangements are I place to allow individuals  to access information that is held about them and  to correct any factual inaccuracies? |  |
| What arrangements are in place for training staff in  their data protection responsibilities? |  |
| Is there a data protection breach policy in place? |  |

**Anonymised data**: is data that is rendered anonymous in such a way that the data subject is not or no longer identifiable. The data must be stripped of any identifiable information making it impossible to derive insights on a discreet individual, even by the party that is responsible for the anonymization.

**Psuedonmysied Data:** the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information. Holding the de-identified data separately from the “additional information” allows the data to only become identifiable when both elements are held together.

**STAGE 3- Address Privacy Risks and Identify Solutions**

|  |  |  |
| --- | --- | --- |
| **Privacy Risk** | **Risk Score**  Impact x likelihood | **Solutions/ Mitigating Actions** |
|  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Impact** | **Negligible (1)** | **Minor (2)** | **Moderate (3)** | **Major (4)** | **Extreme (5)** |
| **Almost Certain (5)** | **5** | **10** | **15** | **20** | **25** |
| **Likely (4)** | **4** | **8** | **12** | **16** | **20** |
| **Possible (3)** | **3** | **6** | **9** | **12** | **15** |
| **Unlikely (2)** | **2** | **4** | **6** | **8** | **10** |
| **Rare/Remote (1)** | **1** | **2** | **3** | **4** | **5** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**STAGE 4: Produce DPIA report**

**(Consult DPO for advice if required** [**dpo@tuh.ie**](mailto:dpo@tuh.ie) **)**

**STAGE 5: Incorporate DPIA Outcomes into DPA Agreement**

|  |  |  |
| --- | --- | --- |
| **Outcome** | **Y** | **N** |
| DPIA incorporated into DPA |  |  |
| Project requires Data Protection Agreement/ Data Sharing Agreement/ EU Model Clause Agreement, Privacy Shield |  |  |
| DPIA added to appendix of above |  |  |
| Clinical Trial Agreement/Research Collaboration Agreement |  |  |

**DPO Review and Advice**

Overall Study risk rating High Medium Low

|  |  |
| --- | --- |
| **DPO Name** |  |
| **Date** |  |
| **Signature** |  |

**Sign off**

**DPIA prepared by:**

|  |  |
| --- | --- |
| **Name** |  |
| **Date** |  |
| **Signature** |  |

**DPIA Sign off Data Controller/ Owner/ Director**

|  |  |
| --- | --- |
| **Name** |  |
| **Date** |  |
| **Signature** |  |

**DPO advice overruled/ not accepted by whom\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Explain reason for rejection:**