**Data Protection Impact Assessment (DPIA) for Health and Social Care Research**

**For consultation and review by the SVUH DPO**

A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimise these risks as far and as early as possible (Data Protection Commission).

The Health Research Regulations ***Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018*** state that in order for research to be conducted researchers must:

* Have ethical approval or be seeking ethical approval
* Specify **controllers** and **processors** and anyone providing funding
* State where the data will be shared
* Be trained in Data Protection
* Demonstrate Data Minimisation compliance and specify the Access controls in place to protect personal data
* Identify the security measures in place to protect the personal data
* Put arrangements in place to anonymise, archive or destroy personal data once research has been completed
* Have transparency in place for participants to understand what is happening to their data, and why
* Obtain explicit consent form participants (unless exempt)

St Vincent’s University Hospital Data Protection Officer will review the content of this document in line with the data protection principles of:

* Lawfulness, fairness and transparency
* Purpose limitation
* Data minimisation
* Accuracy
* Storage limitation
* Integrity and confidentiality (security)
* Accountability

Therefore, it is essential that you fully complete each question and that any questions which may be similar in other documents match the answers in this document

**Sections 1-5:**

Section 1 - Initial Detail's

Section 2 – Full Assessment and Information Flows

Section 3 – Information Audit

Section 4 – Legal Basis for Processing

Section 5 - Consent

Section 6 - Assessment Questions for Processing Personal Data

Section 7 - Risk and Risk Mitigation

DPO Advice

**SECTION 1 – INITIAL DETAILS**

|  |  |  |
| --- | --- | --- |
| * 1. **– THIS PROJECT REQUESTS THE USE OF PERSONAL DATA CURRENTLY HELD BY ST VINCENTS UNIVERSITY HOSPITAL**   *Please tick this box if you will be using St Vincents University Hospital data whether it is identifiable, pseudonymised or anonymised.* | |  |
| * 1. **– TITLE OF THE RESEARCH STUDY** | | |
|  | | |
| * 1. **– PLEASE PROVIDE A BRIEF SUMMARY OF THE STUDY BACKGROUND AND NEED FOR THE STUDY.**   *Please ensure the language used in your answer is at a level suitable for use in a research participant information leaflet.* | | |
|  | | |
| **1.5 – PRINCIPAL INVESTIGATOR IN THE ST VINCENTS UNIVERSITY HOSPITAL** | | |
| **Name** |  | |
| **Title** |  | |
| **Department** |  | |
| **E-Mail** |  | |
| **Phone** |  | |

**SECTION 2 – FULL ASSESSMENT AND INFORMATION FLOWS**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **2.1 – IS THIS A MULTI-SITE STUDY?** | | | Yes | | | | No |
| **2.2 – IF YES, PLEASE SUBMIT A LIST OF ALL SITES PARTICIPATING IN THE STUDY.** | | | | | | | |
|  | | | | | | | |
| **2.3 – IF YES, PLEASE OUTLINE WHAT ARRANGEMENTS WILL BE IN PLACE BETWEEN SVUH AND THE OTHER SITES.**  *(e.g. Controller to Processor agreement, data sharing agreement and material transfer agreement, MOU)* | | | | | | | |
|  | | | | | | | |
| **2.4 – IS THIS RESEARCH OR CLINICAL TRIAL?** | | | | | | | |
| Research | Clinical Trial | | | Other (please specify below) | | | |
|  | | | | | | | |
| Retrospective research | | Prospective research | | | Both | | |
| **2.5 – WHAT IS THE ANTICIPATED START DATE OF THE STUDY?** | | | **2.6 – WHAT IS THE ANTICIPATED DURATION OF THE STUDY (OR THE END DATE)?** | | | | |
|  | | |  | | | | |
| **2.7 – LIST ALL STAKEHOLDERS IN THIS PROJECT, AND THEIR ROLE. DESCRIBE THE RESPONSIBILITIES OF THE STAKEHOLDERS.**  *(This includes any person who has provided funding for, or otherwise supports the research)*  *(The role should also include if the organisation is commercial, not-for-profit, academic, public etc.)* | | | | | | | |
| **Organisation / Name** | **Role** | | | | | **Controller / Processor** | |
|  |  | | | | |  | |
|  |  | | | | |  | |
|  |  | | | | |  | |
|  |  | | | | |  | |
|  |  | | | | |  | |
|  |  | | | | |  | |
|  |  | | | | |  | |
|  |  | | | | |  | |
|  |  | | | | |  | |
|  |  | | | | |  | |
| *A* ***Data******Controller*** *is a person or organisation who decides why data is being collected and exactly how it will be used. (purpose and means)*  *A* ***Data******Processor*** *is a person or organisation who will process data under the strict instruction of a Data Controller. (This person cannot be a direct employee of that Data Controller)* | | | | | | | |
| **2.8 – HAS EVERYBODY INVOLVED IN THE HEALTH RESEARCH STUDY RECEIVED TRAINING IN DATA PROTECTION AND ARE THEY AWARE OF THEIR DATA PROTECTION OBLIGATIONS?** *(please explain)* | | | | | | | |
|  | | | | | | | |
| **2.9 – WHAT AGREEMENTS ARE REQUIRED TO SHARE DATA WITH THE ORGANISATION NAMED ABOVE?** *(Contract, Data Sharing Agreement, Data Processing Agreement etc.)* | | | | | | | |
|  | | | | | | | |
|  | | | | | | | |
| **2.11 – ARE THERE ANY STANDARDS APPLICABLE TO THE PROCESSING?** *Include codes of conduct, protocols, data protection certifications etc.* | | | | | | | |
|  | | | | | | | |
| **2.12 – POTENTIAL RISKS:** *Prior to carrying out the assessment questions section, are there any privacy impacts or risks that have already been identified? How will this impact upon the data subjects?* | | | | | | | |
|  | | | | | | | |
| **2.13 – POTENTIAL BENEFITS:** *Identify the benefits of this initiative in relation to the data subjects. How will this processing benefit the data subjects?* | | | | | | | |
|  | | | | | | | |

**SECTION 3 – INFORMATION AUDIT**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **3.1 – PERSONAL & Special Category DATA:** *What data will be collected / processed?* | | | **3.2 – JUSTIFICATION / PROCESSING ACTIVITY:**  *Why does this data need to be collected? Is there anything you can omit if not necessary?* | | |
| Name | |  |  | | |
| Address | |  |  | | |
| Postcode | |  |  | | |
| Date Of Birth | |  |  | | |
| Age / Year of Birth | |  |  | | |
| Gender | |  |  | | |
| E-Mail Address | |  |  | | |
| Phone Number | |  |  | | |
| Location Data (IP Address) | |  |  | | |
| Health Identifier (or similar) | |  |  | | |
| Education / Employment | |  |  | | |
| Income / Expenses | |  |  | | |
| Lifestyle / Social circumstances | |  |  | | |
| Physical description | |  |  | | |
| Racial / Ethnic origin | |  |  | | |
| Religion or other beliefs | |  |  | | |
| Sex life or sexual orientation | |  |  | | |
| Health data | |  |  | | |
| Genetic Data | |  |  | | |
| Biometric Data | |  |  | | |
| Convictions or offences | |  |  | | |
| Trade Union Membership | |  |  | | |
| Photography, audio or video (details) | |  |  | | |
| Other (please specify) | |  |  | | |
| Other (please specify) | |  |  | | |
| **Number of participants** | | ☐ |  | | |
| **3.3 – WHERE ARE YOU OBTAINING THE DATA (select all that apply)** | | | | | |
| Health Record | Data subject | | | Another source *(specify)* |  |
| **3.4 – AT WHAT STAGE OF THE STUDY WILL THE DATA BE IDENTIFIABLE, PSEUDONYMISED, ANONYMISED?**  *For each of the 3 stages please explain the process and who will be responsible for each process.*  *At what stage will the data be identifiable?*  *At what stage will the data be pseudonymised – who will do this and who will hold the key?*  *At what stage will the data be anonymised – who will do this?* | | | | | |
| **IDENTIFIABLE DATA** | | | | | |
|  | | | | | |
| **PSEUDONYMISED** | | | | | |
|  | | | | | |
| **ANONYMISED** | | | | | |
|  | | | | | |

|  |
| --- |
| **Mapping the information flows** of the research project is required to identify where privacy risks may occur and identify the source and journey of the information as it travels through the system. At this stage one should consider privacy of the information in terms of:   * collection * use * quality * security * disclosure * access and correction * retention * storage and disposal   Understanding the life cycle of information, from collection to disposal, will determine where risks to privacy could occur. |
| Please map the data flows; |

**SECTION 4 – LEGAL BASIS FOR PROCESSING**

|  |  |
| --- | --- |
| **4.1 – LEGAL BASIS FOR PROCESSING PERSONAL DATA:** *(from Article 6 of GDPR)* | |
|  | 1. Consent from the data subject |
|  | 1. Necessary for the performance of a contract |
|  | 1. Necessary for the compliance with a legal obligation to which the controller is subject |
|  | 1. Necessary to protect the vital interests of the data subject |
|  | 1. Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller |
|  | 1. Legitimate interests pursued by the controller or by a third party |

|  |  |
| --- | --- |
| **4.2 – LEGAL BASIS FOR PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA:** *(from Article 9 of GDPR)* | |
|  | 1. Explicit consent from the data subject |
|  | 1. Necessary for employment, social security and social protection law |
|  | 1. Necessary to protect the vital interest of the data subject or another person where the data subject is physically or legally incapable of giving consent |
|  | 1. Legitimate activities with political, philosophical, religious or trade union aim |
|  | 1. Processing relates to personal data which are manifestly made public by the data subject |
|  | 1. Necessary for legal claim or judicial purposes |
|  | 1. Substantial public interest on the basis of EU or Irish law |
|  | 1. Provision of health care – preventative or occupational medicine, for the assessment of working capacity of an employee, medical diagnosis, provision of medical care, treatment or social care, management of health or social care systems and services, or pursuant to a contract with a health practitioner |
|  | 1. Public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices on the basis of EU or Irish law |
|  | 1. Archiving purposes in the public interest, scientific or historical research purposes of statistical purposes |

**SECTION 5 – CONSENT**

|  |  |  |
| --- | --- | --- |
| **5.1 – HOW ARE YOU RECRUITING THE RESEARCH PARTICIPANTS?** | | |
|  | | |
| **5.2 – WILL THIS STUDY INCLUDE CHILDREN OR PATIENTS WHO MAY LACK THE CAPACITY TO CONSENT TO THIS STUDY?** | Yes | No |
| **5.3 – IF YOU ANSWERED YES TO 5.2, PLEASE EXPLAIN YOUR ANSWER.** | | |
|  | | |
| **5.4 – ARE YOU OBTAINING INFORMED CONSENT FROM THE PARTICIPANTS?** | Yes | No |
| **5.5. – IF YOU ANSWERED YES TO 5.4, PLEASE OUTLINE THE CONSENT PROCESS IN FULL. HOW WILL IT BE OBTAINED, WHEN, AND BY WHOM?** | | |
|  | | |
| **5.6 – IF YOU ANSWERED NO TO 5.4, PLEASE JUSTIFY YOUR ANSWER.** *(Consent will be required unless you are applying for a* ***‘Consent Declaration’****)* | | |
|  | | |

**SECTION 6 – ASSESSMENT QUESTIONS FOR PROCESSING PERSONAL DATA**

|  |  |  |
| --- | --- | --- |
| 6.1 – HOW HAVE YOU ENSURED THAT THE RESEARCH PARTICIPANTS ARE FULLY INFORMED AS TO WHAT IS HAPPENING WITH THEIR DATA AND THAT THEY HAVE BEEN TOLD ABOUT THEIR DATA PROTECTION RIGHTS? Participants data protection rights include the right to:   * + - withdraw consent     - access their data     - have inaccurate information rectified     - erasure     - restriction of processing     - data portability   *You must ensure that you can demonstrate this.*  *This could be information leaflets, privacy statements etc.* | | |
|  | | |
| *The principle of ‘purpose limitation’ is to ensure that the reasons for processing are clear and open, and in line with the reasonable expectations of the individuals concerned.*  **6.2 - HOW WILL YOU ENSURE THAT THE DATA COLLECTED WILL NOT BE FURTHER USED IN WAYS THAT ARE INCOMPATIBLE WITH THE ORIGINAL PURPOSE?** | | |
|  | | |
| 6.3 - HOW CAN YOU ENSURE THE ACCURACY OF YOUR DATA?  *Explain the procedures in place to detect/correct inaccurate data.* | | |
|  | | |
| 6.4 – WHERE WILL THE DATA BE PROCESSED / STORED?  *Include the physical location for the data and the media used for storing the data.* | | |
|  | | |
| 6.5 – WHO WILL HAVE ACCESS TO THE DATA AND HOW WILL YOU CONTROL THAT ACCESS? | | |
|  | | |
| 6.6 – LIST THE DATA SUPPORTING ASSETS (HARDWARE, SOFTWARE, NETWORKS, PEOPLE, PAPER OR PAPER TRANSMISSION CHANNELS): | | |
|  | | |
| 6.7 – WHAT SECURITY MEASURES ARE IN PLACE TO PROTECT THE IDENTIFIABLE DATA?  *Will the data be encrypted and/or pseudonymised?* | | |
|  | | |
| 6.8 – WILL PERSONAL DATA BE TRANSFERRED TO A THIRD COUNTRY OR INTERNATIONAL ORGANISATION OUTSIDE OF THE EU? This includes any affiliates of Data Controllers or Data Processors listed in Section 2. *If yes, provide details. Suitable conditions include Adequate jurisdiction, Standard Contract Clauses, Binding Corporate Rules or Authorisation from the Data Protection Commissioner.* | Yes | No |
|  | | |
| 6.9 - ON COMPLETION OF THE STUDY HOW LONG WILL THE DATA BE RETAINED? -- WHY? | | |
|  | | |
| 6.10 - IN WHAT FORMAT WILL THE DATA BE RETAINED? -- WHY? | | |
|  | | |
| 6.11 - WHAT IS THE PROCESS FOR DESTROYING THE DATA ONCE THE RETENTION PERIOD HAS BEEN REACHED? | | |
|  | | |

**SECTION 7 – RISK AND RISK MITIGATION**

For each of the suggested risks below please indicate the likelihood of the risk vs the impact it would have to the rights and freedoms of individuals should the risk occur.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  | **IMPACT** | | | | |
|  |  | **1 -**  **Negligible** | **2 -**  **Minor** | **3 -**  **Moderate** | **4 -**  **Major** | **5 -**  **Critical** |
| **LIKELIHOOD** | **1 - Rare** | **1** | **2** | **3** | **4** | **5** |
| **2 – Unlikely** | **2** | **4** | **6** | **8** | **10** |
| **3 – Possible** | **3** | **6** | **9** | **12** | **15** |
| **4 – Likely** | **4** | **8** | **12** | **16** | **20** |
| **5 – Almost Certain** | **5** | **10** | **15** | **20** | **25** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **7.1 – RISK TABLE** | | | | |
| **No.** | **Data Protection Risk** | **Risk Score** | **Mitigation** | **Post Mitigation Score** |
| **PR1** | Data subjects have not been given enough information about the research or there was insufficient justification for the collection or processing of data. (The processing may not be Lawful, fair and transparent) |  | Detail |  |
| **PR2** | Data subjects cannot exercise ALL of their data protection rights. |  |  |  |
| **PR3** | More data that is necessary is being collected.  (The principal of data minimisation has not been used) |  |  |  |
| **PR4** | Not enough measures in place to ensure the accuracy of the data being processed. |  |  |  |
| **PR5** | Unauthorised access to data or access controls inadequate. |  |  |  |
| **PR6** | Unjustified or unauthorised transfer of data.  Data sharing agreement not in place for all stakeholders. |  |  |  |
| **PR7** | Unjustified or unauthorised transfer of data outside of the EEA Proper contracts not in place or suitable conditions for transfer |  |  |  |
| *The risks above are not intended to be a definitive list. Your project may have specific risks associated with the processing. Please include these as additional supporting documents and indicate this in the check list. You will need to score the risk and state if it is acceptable or include suitable measure that you will implement in order to minimise or mitigate the risk.* | | | | |

|  |
| --- |
| **7.2 – Use this section to discuss any of the privacy risks to the ‘rights and freedoms’ of the research participants.**  **Are the risks at an acceptable level?** |
|  |

**SECTION 8 – DPO Advice / REC comments.**

|  |
| --- |
| **Summary of DPO advise:** |
|  |