|  |  |
| --- | --- |
| NB: Retrospective chart reviews must be completed by health professional directly involved in the care of the service user. | |
|  | |
| Section A: Background Information | |
| Project Name |  |
| Organisation/Department |  |
| Assessment Completed By |  |
| Job Title |  |
| Date completed |  |
| Phone/Mobile |  |
| E-mail |  |
|  |  |
| A(1) Project/Change Outline: What is it that is being planned? If you have already produced this as part of the project's Project Initiation Document or Business Case or Research Application etc. you may make reference to this, however a brief description of the project/process being assessed is still required (in plain English). | |
|  | |
| A(2) Purpose / Objectives: Why is the DPIA being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the project. | |
|  | |
| A(3) What is the purpose of collecting the information within the system? For example, service user treatment, service user administration, research, audit, reporting, staff administration etc. | |
|  | |
| A(4) What are the potential privacy impacts of this proposal?: How will this change impact upon the service users, visitors, volunteers and staff? Provide a brief summary of what you feel these could be, it could be that specific information is being held that hasn't previously or that the level of information about an individual is increasing. | |
|  | |
| A(5) Provide details of any previous Privacy Impact Assessment or other form of personal data compliance assessment done on this initiative. If this is a change to an existing system, a PIA may have been undertaken during the project implementation. | |
|  | |
| A(6) Stakeholders: Who is involved in this project/change? Please list stakeholders, including internal, external, organisations (public/private/third) and groups that may be affected by this system/change. | |
|  | |

|  |  |  |  |
| --- | --- | --- | --- |
| Section B: The Data Involved  *What data is being collected, shared or used?*  *(If there is a chart or diagram to explain attach it as an appendix)* | | | |
|  | **Data Type** - Information that identifies the individual and their personal characteristics | Tick as appropriate | **Justifications –** there must be justification for collecting the particular items and these must be specified here – consider which data items you could remove, without compromising the needs of the project? |
| B(1) | Name |  |  |
| Address |  |
| Postcode |  |
| D.O.B. |  |
| Age |  |
| Gender |  |
| Sexual Orientation |  |
| Racial/ethnic origin |  |
| Tel no. |  |
| Physical description |  |
| MRN |  |
| Mobile/home phone no. |  |
| Email address |  |
| B(2) | 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) |  |  |
| B(3) | Information relating to the individual’s sex life. |  |  |
| B(4) | Information relating to the individual’s sexual orientation |  |  |
| B(5) | Information relating to the family of the individual and the individual’s lifestyle and social circumstances |  |  |
| B(6) | Information relating to any offences committed or alleged to be committed by the individual |  |  |
| B(7) | Information relating to criminal proceedings, outcomes and sentences regarding the individual |  |  |
| B(8) | Information which relates to the education and any professional training of the individual |  |  |
| B(9) | Employment and career history |  |  |
| B(10) | Information relating to the financial affairs of the individual |  |  |
| B(11) | Information relating to the individual’s religion or other beliefs |  |  |
| B(12) | Information relating to the individual’s membership of a trade union. |  |  |
| B(13) | **Will the information be**  Anonymised |  | Select the appropriate choice. Please note that where possible information should be anonymised.  *If the data will be pseudonymised or anonymised at what point after collection will this happen.* |
| Pseudonymised |  |
| Identifiable |  |

|  |
| --- |
| Section C : Assessment |

|  |  |  |
| --- | --- | --- |
| Legal Compliance - is it fair and lawful? | | |
|  | **What is the legal basis for processing the information?** This is your valid legal reason for processing. These reasons are laid out in Article 6 & 9 of GDPR. Any processing of special categories of data such as health, genetic and biometric information will require TWO legal basis for processing - one from Article 6 and one from Article 9. | |
| Answer |  | |
|  | i) - Is the processing of individual’s information likely to interfere with the ‘right to privacy’ under Article 8 of the Human Rights Act?  ii) - Have you identified the social need and aims of the initiative and are the planned response actions proportionate in response to social need? | |
| Answer | **i)** | **ii)** |
|  | It is important that patients affected by the initiative are informed as to what is happening with their information. Is this covered by fair processing information already provided to individuals or is a new or revised communication needed? | |
| Answer |  | |
|  | If you are relying on consent to process personal data, how will consent be obtained and recorded, what information will be provided to support the consent process and what will you do if permission is withheld or given but later withdrawn? | |
| Answer |  | |

|  |  |
| --- | --- |
| Purpose | |
|  | Does the project involve the use of existing personal data for new purposes? |
| Answer |  |
|  | Are potential new purposes likely to be identified as the scope of the project expands? |
| Answer |  |

|  |  |
| --- | --- |
| Adequacy | |
|  | Is the information you are using likely to be of good enough quality for the purposes it is used for? |
| Answer |  |

|  |  |
| --- | --- |
| Accurate and up to date | |
|  | Are you able to amend information when necessary to ensure currency and accuracy? |
| Answer |  |
|  | How are you ensuring that personal data obtained from individuals or other organisations is accurate? |
| Answer |  |

|  |  |
| --- | --- |
| Retention | |
|  | What are the retention periods for the personal data and how will this be implemented? |
| Answer |  |
|  | Are there any exceptional circumstances for retaining certain personal data for longer than is necessary? |
| Answer |  |
|  | How will personal data be fully anonymised or destroyed after it is no longer necessary or fit for purpose? |
| Answer |  |

|  |  |
| --- | --- |
| Rights of the individual | |
|  | How will you action requests from individuals (or someone acting on their behalf) for access to their personal information once held? Will the information be provided to the data subject on their right to rectification, erasure, portability etc? |
| Answer |  |

|  |  |
| --- | --- |
| Appropriate technical and organisational measures | |
|  | What procedures are in place to ensure that all staff with access to the patient data have received adequate information governance training? |
| Answer |  |
|  | If using an electronic system to process subject access requests, what security measures are in place? |
| Answer |  |
|  | How will the information be provided, collated and used? |
| Answer |  |
|  | What security measures will be used to transfer the identifiable information?  Have you identified any potential risk?  The potential impact of any such risk on the data subject.  The likelihood and severity of any risk.  How you intend to deal with it. |
| Answer |  |

|  |  |
| --- | --- |
| Transfers both internal and external including outside of the EEA | |
|  | Will individual’s personal information be disclosed internally/externally in identifiable form and if so to whom, how and why? |
| Answer |  |
|  | Will personal data be transferred to a country outside of the European Economic Area? If yes, what arrangements will be in place to safeguard the personal data? |

|  |  |
| --- | --- |
| Consultation – link back to the stakeholders (A6) | |
|  | Who should be consulted to identify privacy related risks and how will this be achieved? Identify both internal and external stakeholders. |
| Answer |  |
|  | Following the consultation – what privacy risks have been raised? E.g. Legal basis for collecting and using the information, security of the information in transit etc.  You should also include consultation with the data subject – have their views been sought? |
| Answer |  |

|  |  |
| --- | --- |
| Guidance used | |
|  | List any national guidance applicable to the initiative that is referred to. |
| Answer |  |

**Section D: Privacy issues identified and risk analysis**

Table 1 – Identify the privacy and related risks. (See Appendix 1 for further information)

| Ref No. | **Privacy issue –** element of the initiative that gives rise to the risk | **a) Risk to individuals**  (complete if appropriate to issue or put not applicable) | **b) Compliance risk**  (complete if appropriate to issue or put not applicable) | **c) Associated organisation /corporate risk**  (complete if appropriate to issue or put not applicable) |
| --- | --- | --- | --- | --- |
| *PR1* | *Individuals are not aware of the initiative as no communication materials have been planned* | *Individuals not aware that their data is being processed* | *Non-compliance with Article 5(1) principle /Concept 1 – fairness, lawfulness and transparency* | 1. *May lead to public mistrust* 2. *May lead to sanction by the (ODPC)* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 2 – Identify the privacy solutions

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Ref No.** | **Risk – taken from column (a), (b) and/or (c) in table 1.** | **Risk score – see tables at Appendix 2** | | | **Proposed solution(s)**  **/mitigating action(s)** | **Result: is the risk accepted, eliminated, or reduced?** | **Risk to individuals is now OK?**  **Signed off by?** |
| **Likelihood** | **Impact** | **RAG** **status** |  |  |  |
| *PR1* | *Individuals not aware that their data is being processed*  *Non-compliance with DPA principle 1 – fair and lawful processing*  *1. May lead to public mistrust*  *2. May lead to sanction by the ODPC* | 5 | 5 | **25** | *Communication plan to be developed to ensure compliance with fair and lawful processing*  *Assurance that there will be an active communication campaign*  *All relevant staff informed of need to understand and disseminate communication material.* | *Reduced to an acceptable level (it is not possible to eliminate at this stage as the Comms plan will need to ensure it addresses all aspects to enable individuals to be fully informed.* | *Yes*  *Sign-off tbc* |
|  |  |  |  |  |  |  |  |

### 

### Integrate the PIA outcomes back into the project plan

NB. This must include any actions identified in Table 1 and Table 2.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Who is responsible for integrating the PIA outcomes back in to the project plan and updating any project management paperwork? Who is responsible for implementing the solutions that have been approved? Who is the contact for any privacy concerns which may arise in the future?** | | | | | | | |
| **Ref No.** | **Action to be taken** | **Date for completion of actions** | **Anticipated risk score following mitigation** | | | **Responsibility for action – *job title not names*** | **Current status/progress** |
| **Likelihood** | **Impact** | **RAG status** |
| *PR1* | *Communications plan to be developed* |  | *2* | *2* | *4* | *Project Manager to liaise with Communication lead and embed into project plan* | *Meeting arranged with Communication Lead* |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

# Appendix 1: Types of privacy risk

## Risks to individuals

1. Inadequate disclosure controls increase the likelihood of information being shared inappropriately.
2. The context in which information is used or disclosed can change over time, leading to it being used for different purposes without people’s knowledge.
3. New surveillance methods may be an unjustified intrusion on their privacy.
4. Measures taken against individuals as a result of collecting information about them might be seen as intrusive.
5. The sharing and merging of datasets can allow organisations to collect a much wider set of information than individuals might expect.
6. Identifiers might be collected and linked which prevent people from using a service anonymously.
7. Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.
8. Collecting information and linking identifiers might mean that an organisation is no longer using information which is safely anonymised.
9. Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, presents a greater security risk.
10. If a retention period is not established information might be used for longer than necessary.

## 

## Examples of Compliance Risk

1. Non-compliance with the common law duty of confidentiality
2. Non-compliance with the Data Protection Acts 1988 & 2003/ General Data Protection Regulation (GDPR).
3. Non-compliance with the Privacy and Electronic Communications Regulations (PECR)/e-Privacy Regulation.
4. Non-compliance with sector specific legislation or standards e.g. Health Information and Quality Authority (HIQA), Health and Safety Authority (HSA).
5. Non-compliance with human rights legislation United Nations Declaration on human Rights (UNDHR).

## Associated organisation/corporate risk

1. Non-compliance various legislation can lead to sanctions, fines and reputational damage.
2. Problems which are only identified after the project has launched are more likely to require expensive fixes.
3. The use of biometric information or potentially intrusive tracking technologies may cause increased concern and cause people to avoid engaging with the organisation.
4. Information which is collected and stored unnecessarily or is not properly managed so that duplicate records are created, is less useful to the business.
5. Public distrust about how information is used can damage an organisation’s reputation and lead to loss of business.
6. Data losses which damage individuals could lead to claims for compensation.

# Appendix 2: Guidance for completing a risk register

* What is the actual risk? Make sure the risk is clear and concise, well understood and articulated with appropriate use of language, suitable for the public domain.
* Be careful and sensitive about the wording of the risk as risk registers are subject to the Freedom of Information (FOI) requests. This is relevant is your organization is subject to the FOI Act.
* Don’t reference blame to other organisations in the risk register
* Does the risk belong to a business area within your organisation or another body?

It is common to use a RAG matrix rating system for assessing risk. RAG stands for red, amber, green. To achieve a RAG rating, each risk first needs a likelihood and impact score. Each risk will be RAG rated by taking the likelihood and impact scores, and using the matrix below:

Likelihood

Impact

1 - Rare

2 - Unlikely

3 - Possible

4 - Likely

5 – Highly Likely

1 - Negligible

2 - Minor

3 - Moderate

4 - Major

5 - Critical

5

4

9

20

15

12

10

16

8

4

2

1

4

3

2

5

6

8

3

10

6

15

20

12

25

|  |
| --- |
| DPO Feedback |
|  |
|  |
|  |