**St Patrick’s Mental Health Services**

**Data Protection Impact Assessment Policy**

**Relevant Information**

|  |  |
| --- | --- |
| **Title** | Data Protection Impact Assessment Policy |
| **Author** | The Data Protection Office |
| **Publication Date** |  |
| **Superseded Documents** | n/a |
| **Related Documents** | Data Breach Management Policy (DP 0004)  SPMHS Service Provider Confidentiality Agreement  Information Sharing Policy (INFS 0001)  ICT 0001 Security Policy |
| **Version** | 1.0 |
| **SPMHS Data Protection Officer** | John Woods, Data Protection Office, SPMHS, James Street, Dublin 8  **Phone:** +353 1 249 3216  **E-Mail:** [**dpo@stpatsmail.com**](mailto:dpo@stpatsmail.com) |

**Table of Contents**

[1 Introduction 3](#_Toc525634812)

[2 Data Protection Impact Assessments 3](#_Toc525634813)

[3 What are Privacy Risks? 4](#_Toc525634814)

[3.1 Patient / Customer /Staff / Service User Perspective 4](#_Toc525634815)

[4 DPIA Initiation 5](#_Toc525634816)

[4.1 Data Protection Impact Assessment Screening Questions 5](#_Toc525634817)

[4.2 Conducting a Data Protection Impact Assessment (DPIA) 6](#_Toc525634818)

[What should a DPIA include? 6](#_Toc525634819)

[4.3 DPIA Team needed to Complete Template 7](#_Toc525634820)

[4.4 Does my Project Need a DPIA? 7](#_Toc525634821)

[5 Privacy Impact Assessment Template 9](#_Toc525634822)

[5.1 Section 3 – Privacy issues identified and risk analysis 15](#_Toc525634823)

[5.1.1 Identify the privacy and related risks (see Appendix 1 for further information) 15](#_Toc525634824)

[5.1.2 Identify the privacy solutions 17](#_Toc525634825)

[5.1.3 Integrate the PIA outcomes back into the project plan 18](#_Toc525634826)

[6 Appendix 1: Types of privacy risk 19](#_Toc525634827)

[6.1 Risks to individuals 19](#_Toc525634828)

[6.2 Examples of Compliance Risk 19](#_Toc525634829)

[6.3 Associated organisation/corporate risk 19](#_Toc525634830)

[7 Appendix 2: Guidance for completing a risk register 21](#_Toc525634831)

# Introduction

This Data Protection Impact Assessment (hereafter, “DPIA”), describes how St. Patrick’s Mental Health Services (“SPMHS”) employs the use of additional administrative measures to safeguard and protect personal information relating to service users, visitors and staff. The protection of personal information is something SPMHS takes very seriously***. SPMHS undertakes to respect the privacy rights of its staff, service users, volunteers, visitors and will take all necessary steps and measures to protect the fundamental privacy rights and freedoms of individuals.***

At St. Patrick’s Mental Health Services, customers, service users, visitors, applicants, staff, volunteers and other individuals who fall under the category of data subjects, have an expectation that their privacy and confidentiality will be respected at all times, during service provision, patient care and beyond. It is essential consequently that when SPMHS is contemplating or implementing any new initiatives and/or involves the use of new technology, the perceived impact of collection, use and disclosure of any personal data is considered integral to an individual’s privacy. Carrying out a Data Protection Impact Assessment (DPIA) is a disciplined way of achieving this objective.

# Data Protection Impact Assessments

A Data Protection Impact Assessment (DPIA) is a process that helps St. Patrick’s Mental Health Services identify risks to the privacy of data subjects and ensure legitimate best practice are followed when a new project is planned, or when changes are made to an already existing process or service. The purpose that the DPIA serves is to ensure that privacy related risks that arise during data collection, use and disclosure are mitigated using appropriate plans and measures, while allowing the objectives, outputs or deliverables of a project which involves the use of personal data, to be met.

DPIA is principally a useful tool for SPMHS in identifying privacy related risks and ensures that relevant responses are in place to address each identified risk in a timely manner. Instances where a Data Protection Impact Assessment (DPIA) may be required includes but is not limited to:

* Planning a new information sharing initiative such as working with new partners or in different ways;
* Introducing new IT systems for collecting and accessing personal data;
* Intending to use personal data for new uses e.g. Research.

# What are Privacy Risks?

A privacy risk can be defined as the probability that the fundamental rights and freedom of a data subject may be put at risk through the data processing activities of SPMHS. Recital 4 of the General Data Protection Regulation defines the fundamental rights of a data subject as;

* respect for private and family life,
* respect for home and communications,
* protection of personal data,
* freedom of thought, conscience and religion,
* freedom of expression and information….”

Privacy related risks can include one or all of the following:

* Risks to service users, staff, visitors or other third parties (for example, ill-use or overuse of patient or staff data, loss of patient anonymity, intrusion into the private lives of service users, visitors, staff, volunteers and third parties through monitoring activities, lack of transparency, fairness and lawfulness of data processing activities, etc.).
* Compliance risks e.g. breach of the General Data Protection Regulation (GDPR) or other health related legislation
* Inherent or residual risks to SPMHS (for example, project failure and associated costs, legal penalties or claims, damage to Hospital’s reputation, loss of trust of service users or the public).

## Patient / Customer /Staff / Service User Perspective

DPIAs helps SPMHS see things from the data subject’s perspective. Data provided to SPMHS by service users for the purpose of achieving its corporate objective of provision of high class patient care. How patient data is used and why it will be used should be clearly outlined and articulated to the service user and where appropriate, requires that consent is sought, given, maintained and sustained. Where relevant, SPMHS will adopt a “No decision about me, without me” approach as part of its accountability obligations. Understanding the potential impact of personal data processing on service users can enable systems to be designed around data subject’s legal rights and expectations of confidentiality as outlined under the new regulation. This phenomenon is known as data protection by design and default.

A DPIA also checks organisational compliance against legal framework (where relevant).

# DPIA Initiation

A lead person preferably the Data Protection Officer should be nominated to coordinate and lead the DPIA process. A DPIA starts with a screening process. The screening questions are provided in the table below. Answering the screening questions will identify whether or not the proposed initiative will impact on the fundamental rights and freedoms of individuals, which in turn determines whether a DPIA is required or not. The screening questions should be designed in such a way that pointers on the degree, scope and scale of privacy issues being experienced, are provided.

## Data Protection Impact Assessment Screening Questions

Where response(s) to the below questions is or are negative, a DPIA may not be required. Where response to each screening question is either affirmative or unsure, a DPIA may be required.

Should the project initiative change to incorporate informational privacy at any point in the future, the DPIA screening questionnaire would need to be completed again.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Detailing appropriate screening questions that are relevant to SPMHS’s project initiatives will highlight specific and individual privacy considerations that will determine and inform the types of inputs into SPMHS’s corporate risk register. This will also assist in ensuring that proposed investment is proportionate to the risks involved: | | | | | |
|  | | Yes | No | Unsure | Comments |
| 1 | Will information about individuals raise privacy concerns or expectations e.g. health records, criminal records or other information people would consider particularly private? |  |  |  |  |
| 2 | Will project initiative involve collection of new information about service users, visitors or staff? |  |  |  |  |
| 3 | Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used? |  |  |  |  |
| 4 | Will project initiative require use of patient data in ways which they may find intrusive[[1]](#footnote-1)? |  |  |  |  |
| 5 | Will patient data be disclosed to other organisations or people who have not previously had routine access to such? |  |  |  |  |
| 6 | Will project initiative involve using new technology which might be perceived as being privacy intrusive or biased e.g. biometrics or facial recognition? |  |  |  |  |
| 7 | Will project initiative result in SPMHS making decisions or taking actions against individuals in ways which can have a significant negative impact on them? |  |  |  |  |

## Conducting a Data Protection Impact Assessment (DPIA)

## What should a DPIA include?

In simple terms a DPIA should: -

1. articulate in clear terms aims or objectives of project initiative
2. explain why DPIA is necessary (using the initial screening questions will enable this to be quickly identified)
3. document data flows in light of, what data is being processed, source and destination (data inflows and outflows)
4. identify the risks to individual’s privacy in terms of personal data security and access, giving consideration to potential threats to personal data confidentiality, integrity or availability
5. clarify the legal basis for processing including retention threshold where appropriate
6. Identify and evaluate likely or available solutions (how can you reduce or remove the risk?)
7. Sign off and record the DPIA outcomes
8. Integrate the outcomes into the project plan
9. Consult with internal and external stakeholders (including the ODPC where required. This is particularly relevant where processing would result in a high risk regardless of measures taken by DC/DP to mitigate the risk), as needed, throughout the process
10. Consideration should be given to incorporating a minimum of 8 – 14 weeks lead time as it can take even longer for the ODPC to feedback to SPMHS. This among other things, is determined by complexity of the intended processing.

## DPIA Team needed to Complete Template

For the DPIA to be effective it needs input from people with a range of expertise, skills and authority. Important features for members of the team include:

1. An understanding of the project’s aims and the organisation’s culture;
2. Authority to influence the design and development of the project and participate in decision making;
3. Expertise in data protection and compliance matters;
4. Ability to assess and communicate organisational risks;
5. Ability to assess which privacy solutions are feasible for the relevant project; and
6. Ability to communicate effectively with stakeholders and manage expectations.

The DPIA will include but is not limited to the following stakeholders whose input will be sought;

1. Project Sponsor
2. Project Manager
3. Risk Manager
4. Data Protection Officer
5. Project Team

## Does my Project Need a DPIA?

Under GDPR, DPIA is now a legal requirement especially in instances where processing of personal data poses a fundamental risk to the rights and freedoms of individuals. DPIAs may require input from the Data Protection Commissioner especially in situations where processing is complex. This is based on;

1. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by SPMHS which includes but is not limited to
   1. service user evaluation or scoring as a result of profiling and trend analysis;
   2. automated taking decisions on data subjects producing “legal effects that include processing that may lead to the exclusion or discrimination against individuals”
   3. sensitive personal data collection e.g. genetic or biometric data collection
2. an assessment of the necessity and proportionality of the processing operations in relation to defined purpose(s);
3. an assessment of the risks processing poses to the rights and freedoms of service users, volunteers, visitors and staff;
4. measures envisaged to address the risks, including both technical and organisational safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance and accountability with the Regulation, which takes into account the rights and legitimate interests of service users, volunteers, visitors and staff.

Taking into consideration the nature scope of processing as well as criticality of data, DPIA may be suitable for:

1. A new IT system for storing and accessing personal data
2. A proposal to identify people in a particular group or demographic and initiate a course of action
3. Scientific research which involves use of personal data
4. Using existing data for a new and unexpected or more intrusive purpose
5. A new surveillance system (especially one which monitors members of the public) or the application of new technology to an existing system
6. A new database which consolidates information held by separate parts of SPMHS
7. Legislation, policy or strategies which will impact on privacy through the collection of personal information, or through surveillance or other monitoring
8. Data transfers across borders outside the European Union(EU)
9. Long standing databases where the privacy impact may not have been considered previously or the legal or organisational framework has changed and may give rise to new privacy risks or issues.

A single DPIA could be used to assess multiple processing operations that are similar in terms of the risks presented, provided adequate consideration is given to the specific nature, scope, context and purposes of the processing. This might mean where similar technology is used to collect the same sort of data for the same purposes.

Where the processing operation involves joint controllers, they need to define their respective obligations precisely. Their DPIA should set out which party is responsible for the various measures designed to treat risks and to protect the rights of the data subjects.

# Privacy Impact Assessment Template

**Section 1: Background Information**

|  |  |
| --- | --- |
| Project Name |  |
| Organisation/Department |  |
| Assessment Completed By |  |
| Job Title |  |
| Date completed |  |
| Phone/Mobile |  |
| E-mail |  |
| 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 etc. you may make reference to this, however a brief description of the project/process being assessed is still required. | |
|  | |
| Purpose / Objectives: Why DPIA is being undertaken? This could be the objective of the process or the purpose of the system being implemented as part of the project. | |
|  | |
| 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. | |
|  | |
| What are the potential privacy impacts of this proposal? How will this change impact upon the service users, visitors 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. | |
|  | |
| 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. | |
|  | |
| 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 2: 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** | | **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? |
| Information that identifies the individual and their personal characteristics | Name |  |  |
| Address |  |
| Postcode |  |
| Dob |  |
| Age |  |
| Sex |  |
| Gender |  |
| Racial/ethnic origin |  |
| Tel no. |  |
| Physical description |  |
| MRN |  |
| Mobile/home phone no. |  |
| Email address |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Yes** | **N/A** | **Justification** |
| 1. 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) |  |  |  |
| 1. Information relating to the individual’s sex life. |  |  |  |
| 1. Information relating to the individual’s sexual orientation |  |  |  |
| 1. Information relating to the family of the individual and   the individual’s lifestyle and social circumstances |  |  |  |
| 1. Information relating to any offences committed or alleged to be committed by the individual |  |  |  |
| 1. Information relating to criminal proceedings, outcomes and sentences regarding the individual |  |  |  |
| 1. Information which relates to the education and any professional training of the individual |  |  |  |
| 1. Employment and career history |  |  |  |
| 1. Information relating to the financial affairs of the individual |  |  |  |
| 1. Information relating to the individual’s religion or other beliefs |  |  |  |
| 1. Information relating to the individual’s membership of a trade union. |  |  |  |
| Will the information be   1. Anonymised |  |  |  |
| 1. Pseudonymised |  |  |
| 1. Identifiable |  |  |
| Select the appropriate choice. Please note that where possible information should be anonymised |  |  |

**Section 3: Assessment**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Question | Response | Required Action  E.g. Seek Information Governance advice |
| Legal compliance – is it fair and lawful? | 1. 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. |  |  |
| 1. a) - Is the processing of individual’s information likely to interfere with the ‘right to privacy’ under Article 8 of the Human Rights Act?   b) - Have you identified the social need and aims of the initiative and are the planned response actions proportionate in response to social need? |  |  |
| 1. It is important that service users 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? |  |  |
| 1. 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? |  |  |
| Purpose | 1. Does the project involve the use of existing personal data for new purposes? |  |  |
| 1. Are potential new purposes likely to be identified as the scope of the project expands? |  |  |
| Adequacy | 1. Is the information you are using likely to be of good enough quality for the purposes it is used for? |  |  |
| Accurate and up to date | 1. Are you able to amend information when necessary to ensure currency and accuracy? |  |  |
| 1. How are you ensuring that personal data obtained from individuals or other organisations is accurate? |  |  |
| Retention | 1. What are the retention periods for the personal data and how will this be implemented? |  |  |
| 1. Are there any exceptional circumstances for retaining certain personal data for longer than is necessary? |  |  |
| 1. How will personal data be fully anonymised or destroyed after it is no longer necessary or fit for purpose? |  |  |
| Rights of the individual | 1. 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?   . |  |  |
| Appropriate technical and organisational measures | 1. What procedures are in place to ensure that all staff with access to the patient data have received adequate information governance training? |  |  |
| 1. If using an electronic system to process subject access requests, what security measures are in place? |  |  |
| 1. How will the information be provided, collated and used? |  |  |
| 1. What security measures will be used to transfer the identifiable information? 2. Have you identified any potential risk? 3. The potential impact of any such risk on the data subject. 4. The likelihood and severity of any risk. 5. How you intend to deal with it. |  |  |
| Transfers both internal and external including outside of the EEA | 1. Will individual’s personal information be disclosed internally/externally in identifiable form and if so to whom, how and why? |  |  |
| 1. 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 | 1. Who should be consulted to identify privacy related risks and how will this be achieved? Identify both internal and external stakeholders. *Link back to stakeholders on page 3.* |  |  |
| 1. 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? |  |  |
| Guidance used | 1. List any national guidance applicable to the initiative that is referred to. |  |  |

## Section 3 – Privacy issues identified and risk analysis

### Identify the privacy and related risks (see Appendix 1 for further information)

***NB***. By allocating a reference number to each identified privacy issue will ensure you link back to this throughout the rest of the assessment. Column (a), (b) and/or (c) must be completed for each privacy issue identified in column

*Table 1*

| Ref No. | **Privacy issue –** element of the initiative that gives rise to the risk | 1. **Risk to individuals**   (complete if appropriate to issue or put not applicable) | 1. **Compliance risk**   (complete if appropriate to issue or put not applicable) | 1. **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)* |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### Identify the privacy solutions

*Table 2*

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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 |  | *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* |  | *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 with 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.
* 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**



Using the risk “RAG” rating system for scoring risks means risks can be ranked so that the most severe are addressed first. Decisions can then be made as to what mitigating action can be taken to alleviate the risk.

A

A/R

R

R

R

A

A

A/R

R

R

A/G

A

A

A/R

A/R

Very High -5

High - 4

Medium - 3

G

A/G

A/G

A

A

G

G

G

G

G

1

Rare

2

Unlikely

3

Possible

4

Likely

5

Almost Certain

**Likelihood**

Low - 2

Very Low - 1

**Impact**

1. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online and extends to monitoring the records of senders and recipients as well as the content of messages [↑](#footnote-ref-1)