Health
Information
and Quality
Authority

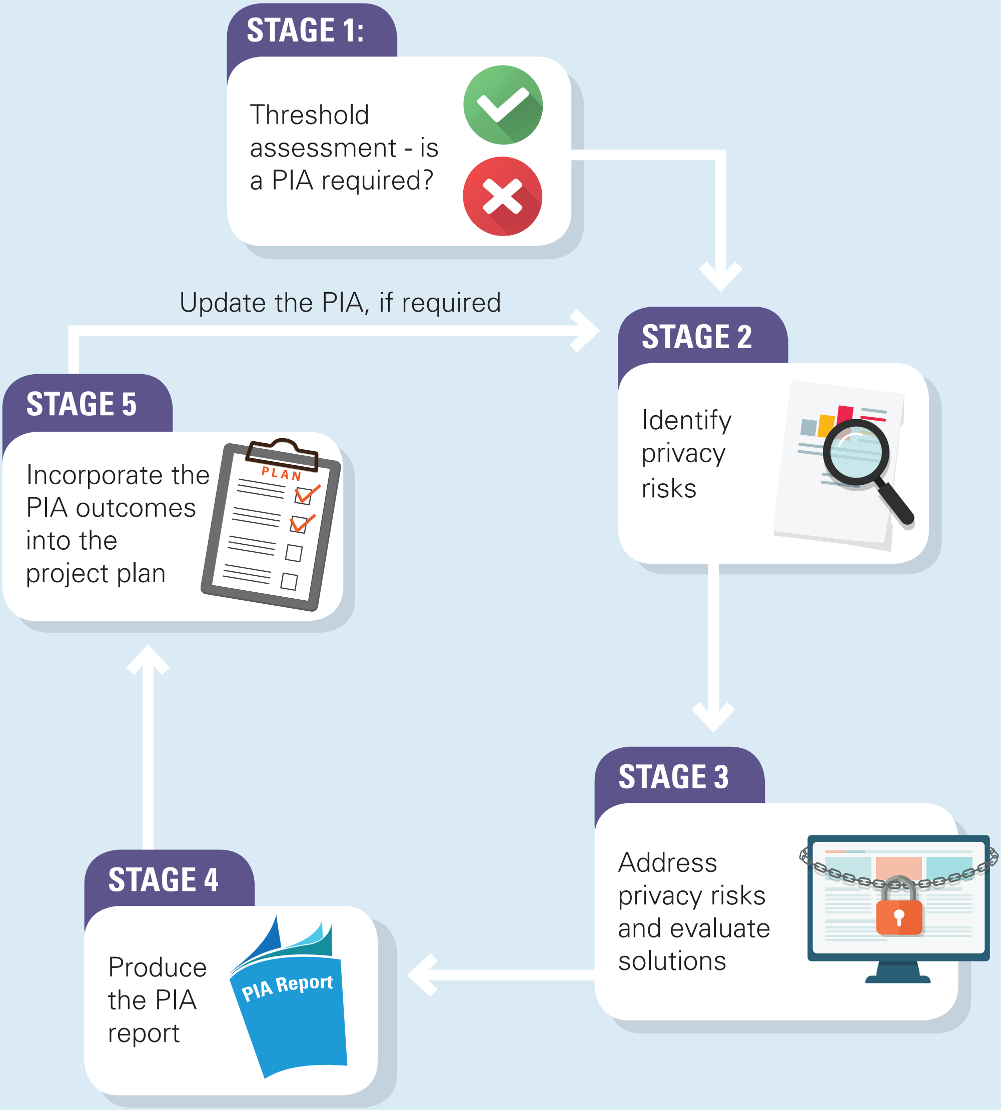
An tÚdarás Um Fhaisnéis
agus Cáilíocht Sláinte

# Privacy Impact Assessment toolkit for health and social care

October 2017

*Safer Better Care*

# The 5 stages of the Privacy Impact Assessment (PIA) process



**STAGE 1:**

Threshold assessment - is a PIA required?

**STAGE 2**

Identify privacy risks

**STAGE 3**

Address privacy risks and evaluate solutions

**STAGE 4**

Produce the PIA report

**STAGE 5**

Incorporate the PIA outcomes into the project plan

Update the PIA, if required

# About the Health Information and Quality Authority

The Health Information and Quality Authority (HIQA) is an independent authority established to drive high quality and safe care for people using our health and social care services in Ireland. HIQA's role is to develop standards, inspect and review health and social care services and support informed decisions on how services are delivered.

Reporting to the Minister for Health and the Minister for Children and Youth Affairs, HIQA has statutory responsibility for:

- **Setting Standards for Health and Social Services**
- **Regulation**
- **Monitoring Children's Services**
- **Monitoring Healthcare Safety and Quality**
- **Health Technology Assessment**
- **Health Information**

# Purpose of this toolkit

This toolkit has been developed to support the health and social care sector in undertaking Privacy Impact Assessments (PIA). The document outlines a high-level summary of each stage of the PIA process and tools that can be used to undertake a PIA.

This toolkit is to be used in conjunction with the *Guidance on Privacy Impact Assessment in Health and Social Care* available on www.hiqa.ie.

**Please note:** The content of this document does not purport to be legal advice or a definitive interpretation of statutory provisions. Any person who requires legal advice should seek this from a suitably qualified legal advisor.

# Key terms used in this document

This section outlines the key terms which are used for the purposes of this toolkit.

**General Data Protection Regulation (GDPR):**

The GDPR comes into effect on 25 May 2018, replacing Irish and EU data protection legislation. New concepts, such as 'data protection by design and default', are legislated for. This means that Privacy Impact Assessments should be used to embed data privacy directly into the design of projects at an early stage.

**Privacy Impact Assessment (PIA):**

A process designed to identify and address the privacy issues of a particular project. It considers the future consequences of a current or proposed action by identifying any potential privacy risks and then examining ways to mitigate or avoid those risks. The term *'Data Protection Impact Assessment (DPIA)'* is used in the GDPR.

**Data Protection Officer (DPO):**

A Data Protection Officer is a designated person appointed by an organisation to advise on data protection practices. Appointing a Data Protection Officer is a requirement for service providers under the GDPR.

### Service provider:

This term is used in this document to describe any agency, practice, hospital, or organisation proposing to undertake a project involving the collection or processing of personal health information. It also refers to an individual if that individual is acting as a legal entity for example; a general practitioner (GP), private consultant or national data collection. Data protection legislation, including the GDPR, refers to the legal term '*Data Controller*'.

### Project:

In this document, a project means any proposal, review, system, programme, process, application, service or initiative that includes the processing of personal health information. The definition also includes any proposed amendment(s) to the items listed above that are already in existence.

### Personal health information:

Personal data relating to the physical or mental health of an individual; including its use for the provision or registration of health and social care services, which reveal information about a person's physical or mental health status.

# Privacy

## What is privacy and why is it important?

Privacy can be defined as 'the right to be left alone'. In terms of personal health information, privacy can be described as the right of individuals to keep their information confidential. Health information is considered to be one of the most sensitive forms of information. Health and social care providers collect, use, store and disclose personal health information in the process of providing safe, effective health and social care. This can present a risk to the privacy and confidentiality of service users as increasing amounts of personal health information are processed.

## Individuals' rights to privacy

Each individual accessing health and social care has specific rights in relation to their privacy. Data protection legislation ensures that the right to privacy is protected by those who collect, use and disclose personal health information. Under legislation, everyone is entitled to:

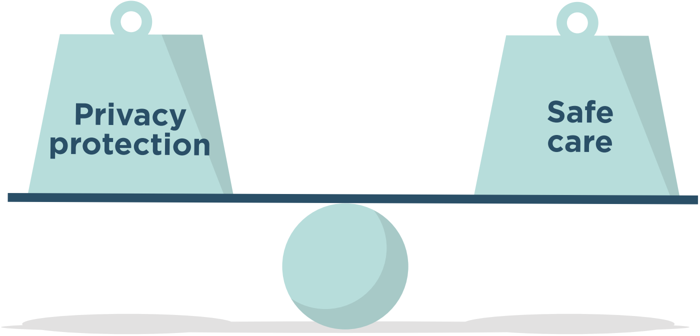
- feel confident that their personal information is kept safely and securely
- check that the information held about them is correct, complete and up to date

- have their information used only for its original stated purpose(s)

- know who can access their personal health information and why
- access and receive a copy of any information held about them
- change any details that are factually incorrect or remove any information that is not held for a valid reason.

## Service provider responsibilities in relation to privacy

Privacy is a human right enshrined in both Irish and European legislation. Service providers are obliged to uphold this human right and respect the privacy and confidentiality rights of individuals in relation their personal health information. Service providers must create a balance between respecting individuals' privacy and providing safe, effective care.



## Data protection legislation

The General Data Protection Regulation (GDPR) comes into effect on 25 May 2018, replacing current Irish and EU data protection legislation. The principles of data protection remain similar: service providers are responsible for ensuring that they only hold personal information that is actually needed; and that they hold it securely, for as long as it is needed, and for the specific purposes for which it was obtained.

In addition, the GDPR puts a greater emphasis on evidence-based compliance, transparency, more extensive rights for data subjects, and stronger penalties for non-compliance. Some principles, such as 'data protection by design' and 'data protection by default', are new. In practice, this means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage.

Under the GDPR, a service provider who processes personal health information must:

- appoint a suitably qualified and experienced Data Protection Officer
- conduct a Data Protection Impact Assessment for the processing of personal health information.

# Privacy Impact Assessment

Conducting a Privacy Impact Assessment (PIA) is fundamental to protect individual privacy. The primary objective of a PIA is to weigh up any negative privacy impacts of a project against the benefits offered to the public.

Privacy Impact Assessments serve as an 'early warning system' for the organisation, detecting potential privacy problems and identifying precautions to be undertaken at the earliest possible stage.

The term 'Privacy Impact Assessment' (PIA) is often used interchangeably with the term 'Data Protection Impact Assessment' (DPIA). However, data protection is only one aspect of privacy. A PIA ensures that privacy is considered as a human right, as well as ensuring compliance with the GDPR obligation of undertaking a DPIA. Therefore, in the context of health and social care, the concepts of both privacy and data protection have been considered and hence the term PIA is used.

## Why are PIAs important?

Privacy Impact Assessments promote trust. They reassure stakeholders, including the public, that the organisation takes privacy seriously and promotes an ethos of transparency and accountability.

Service providers are legally obliged to conduct a PIA to protect the privacy of the individuals whose personal health information they collect. Service providers are fully accountable for carrying out a PIA and documenting it appropriately.

## When should PIAs be conducted?

A PIA should be undertaken and any recommendations to the project design should be implemented, prior to personal health information being processed.

The potential impact on individual privacy should be considered at the start of a project or when proposing a change to an existing project, as risks may be costly to address later on. The size or budget of a project is not a useful indicator of its impact on privacy, as small changes to a current process may impact individual privacy greatly. The PIA should be a ‘live document’ which can be revised as the project develops or changes throughout the project lifecycle.

## Who should be involved?

Consultation with key stakeholders is an important element of the PIA process. This ensures that key privacy issues are noted, addressed and communicated. Consultation allows stakeholders to identify privacy risks based on their own personal experience, expertise or interests. It also provides an opportunity to suggest ways to mitigate these risks.

It is recommended to build consultation into each stage of the PIA process.

Stakeholders include those who are interested in, or may be affected by, the project being considered. Both internal and external stakeholders should be consulted, as needed, throughout the PIA process. Many stakeholder consultation models exist including; surveys, focus groups, interviews and workshops. Careful consideration should be given to which model would be appropriate to gather the information required.

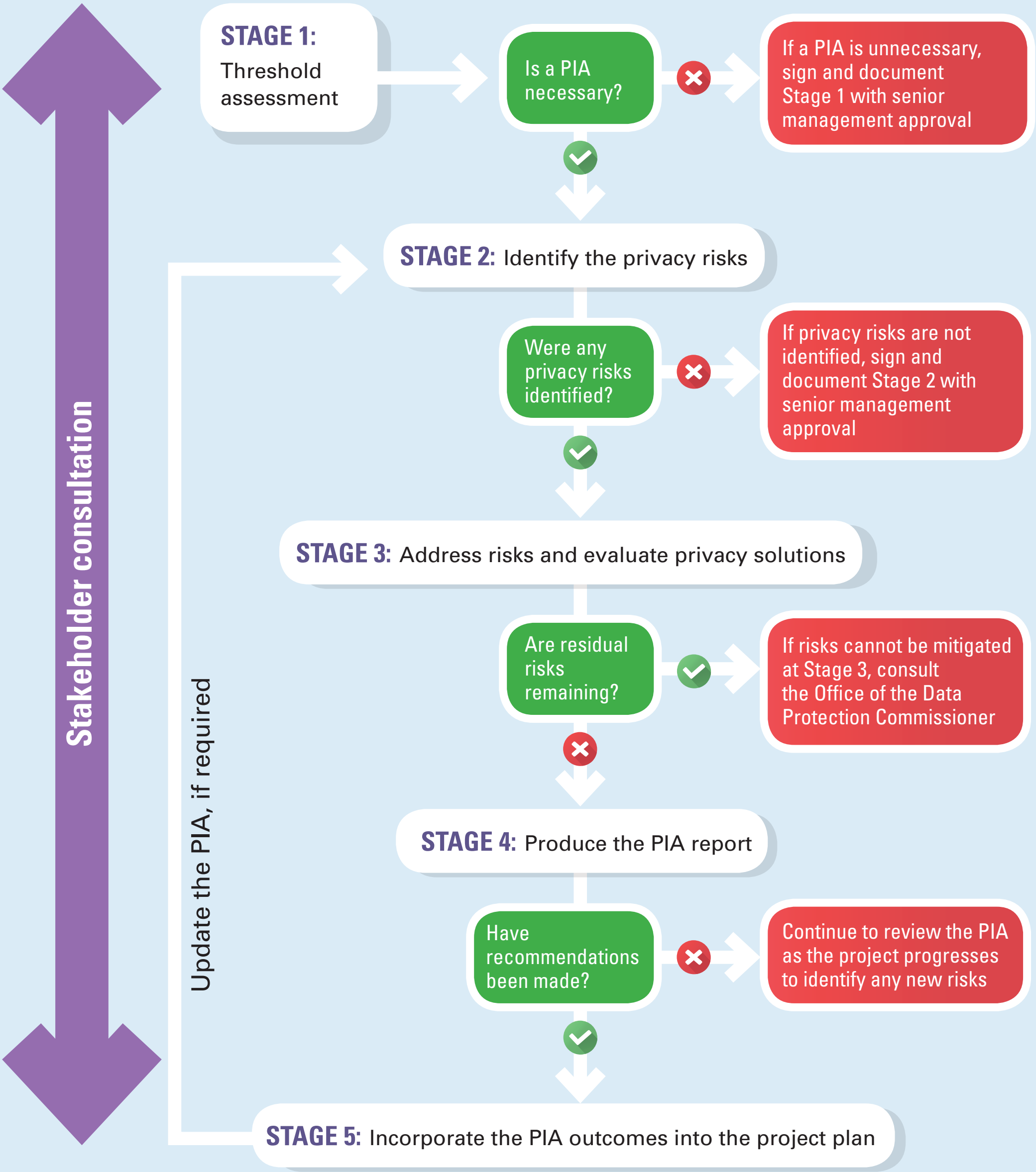
### Examples of key stakeholders for consultation during the PIA process:

**Internal stakeholders:** project team, Data Protection Officer, IT staff, records management personnel, senior management and or the communications team.

**External stakeholders:** service users or their representatives, third party organisations, industry experts and or academics.

## Stages of the PIA process

Each stage of the PIA process must be documented to ensure compliance with the GDPR.



**STAGE 1:** Threshold assessment

Is a PIA necessary?

✗ If a PIA is unnecessary, sign and document Stage 1 with senior management approval

✓

**STAGE 2:** Identify the privacy risks

Were any privacy risks identified?

✗ If privacy risks are not identified, sign and document Stage 2 with senior management approval

✓

**STAGE 3:** Address risks and evaluate privacy solutions

Are residual risks remaining?

✓ If risks cannot be mitigated at Stage 3, consult the Office of the Data Protection Commissioner

✗

**STAGE 4:** Produce the PIA report

Have recommendations been made?

✗ Continue to review the PIA as the project progresses to identify any new risks

✓

**STAGE 5:** Incorporate the PIA outcomes into the project plan

# Stage 1 - PIA threshold assessment

A threshold assessment is a short, initial assessment of a project to determine whether its potential privacy impact requires a PIA. It is a simple tool that should be incorporated into project management processes to ensure that privacy is routinely considered at the beginning of a project. The questions in the threshold assessment checklist determine if a PIA is required, focusing on the scope of the project and how personal health information will be used.

## Who should be involved?

The threshold assessment should be carried out by the project team. Each stage of the PIA process must be documented to ensure compliance with the GDPR.

If the result of the threshold assessment is that a PIA is not required, the process should be documented, with senior management approval, and stored in the project management file.

If the result of Stage 1 is that a PIA is required, consult the designated Data Protection Officer of the organisation for advice. Before undertaking the PIA consider the team required; set out the terms of reference, consider the benefits of conducting the PIA within the organisation or getting an external consultant.

## List of sample questions to be asked as part of a threshold assessment

### Does the project involve:

1. The collection, use or disclosure of personal health information?

2. The collection, use or disclosure of additional personal health information held by an existing system or source of health information?

3. A new use for personal health information that is already held?

4. Sharing of personal health information within or between service providers?

5. The linking, matching or cross-referencing of personal health information that is already held?

6. The creation of a new, or the adoption of an existing, identifier for individuals; for example using a number or biometric?

7. Establishing or amending a register or database containing personal health information?

8. New or innovative use of technology or organisational solutions?

**9.** Exchanging or transferring personal health information outside the European Union?

**10.** The use of personal health information for research or statistics, whether de-identified or not?

**11.** A new or changed system of data handling; for example, policies or practices around access, security, disclosure or retention of personal health information?

**12.** Any other measures that may affect privacy or that could raise privacy concerns with the public?

# Stage 2 – Identify privacy risks

In Stage 2 of a Privacy Impact Assessment, the service provider is required to explore and document the following:

- privacy management arrangements of the service provider
- description of the project
- mapping of information flows.

This section requires the project team to provide an introduction and background to the project including the reasons for undertaking the project. It serves to put the project and any potential risks to individuals' fundamental right to privacy into context. It is imperative to explore the scope of the project to determine how far-reaching its impact is likely to be. Generally, the greater the scope of the project, the more detailed the PIA is likely to be.

**The project description should:**

- Describe the overall aims and objectives of the project.
- Outline the background to the project.
- Examine the scope of the project.
- Provide details of the information governance structures in place.
    - Who is the project lead?
    - Who is the PIA lead?
    - Who is the Information Governance lead?
    - Who is the designated Data Protection Officer of the organisation?
    - Are third party organisations involved? Name those involved and outline the service level agreements that are in place.
- Describe the individuals who will be affected by the project.
- Describe how the project fits into current organisational arrangements.
    - Any links with existing projects or programmes?

## Who should be involved?

The operational aspects of the organisation and project need to be understood in detail to identify privacy risks. A number of key people may need to be consulted including the programme or project manager, IT staff, records management staff, and partner organisations such as third-party service providers or contracted data processors.

If privacy risks are not identified in Stage 2, the process should be documented, with senior management approval, and stored in the project management file.

Each stage of the PIA process must be documented to ensure compliance with the GDPR.

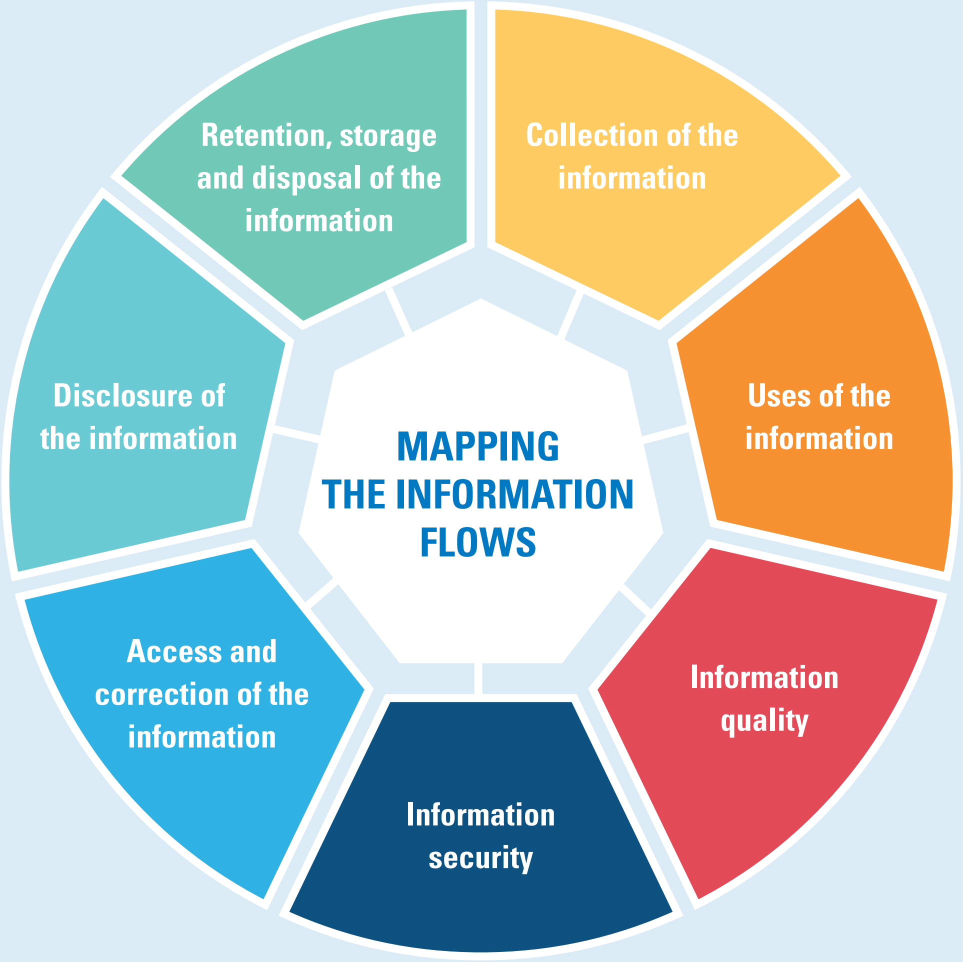
## Mapping information flows

Mapping the information flows of a project is an important step in identifying privacy risks. This stage should consider the privacy of 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, can help determine where risks to privacy could occur.

### Mapping the information flows should examine the following:

- What personal information will be collected?
- Where will the information be sourced?
- How it will be collected?
- How will information be used and disclosed?
- How will the processes ensure the quality of the information collected?
- What are the security safeguards that will be in place?
- What arrangements are in place to allow individuals to access information that is held about them, and to correct any factual inaccuracies?


MAPPING THE INFORMATION FLOWS
Collection of the information
Uses of the information
Information quality
Information security
Access and correction of the information
Disclosure of the information
Retention, storage and disposal of the information

# Stage 3 - Address privacy risks and evaluate solutions

Stage 3 requires the service provider to analyse the privacy risks identified in Stage 2, evaluate privacy solutions, and undertake stakeholder consultation.

Risk analysis:

- is about developing an understanding of privacy risks to the rights and freedoms of individuals
- determines the impact and the likelihood of a risk occurring, both to individuals and to the service provider
- is an ongoing process, and should be repeated when a change in circumstances may affect risk.

The service provider must then evaluate solutions to reduce or eliminate the risk. The positive effects of risk reduction should always be balanced against how the project's goals will be affected. A privacy risk register is a useful tool to record information about the analysis of risk and the evaluation and management of solutions to address the risk.

## Who should be involved?

Service providers are legally required to seek the views of service users or their representatives, where appropriate, on any identified privacy risks and the proposed solutions to address them.

The service provider must consult the Data Protection Commissioner if a 'high risk' cannot be mitigated at Stage 3. If a decision is made to proceed with a project with un-resolved risks, a business case justifying this decision should; outline the public benefit of the project compared to the likely privacy implications for individuals involved, and be documented with senior management approval.

Each stage of the PIA process must be documented to ensure compliance with the GDPR.

## Analyse privacy risks

### Questions to be asked when analysing privacy risks:

- If the event were to occur, what is the likely impact to individuals?
- If the event were to occur, what is the likely impact on the service provider?
- What is the likelihood of the event occurring?

## Privacy risk matrix

A risk matrix is a useful tool for ranking and displaying risks by defining ranges for the likelihood and impact of risks occurring.

| | **Likelihood** | | | | |
|---|---|---|---|---|---|
| **Impact** | Rare 1 | Unlikely 2 | Possible 3 | Likely 4 | Highly likely 5 |
| Negligible - 1 | 1 | 2 | 3 | 4 | 5 |
| Minor - 2 | 2 | 4 | 6 | 8 | 10 |
| Moderate - 3 | 3 | 6 | 9 | 12 | 15 |
| Major - 4 | 4 | 8 | 12 | 16 | 20 |
| Critical - 5 | 5 | 10 | 15 | 20 | 25 |

🟩 **Low (1-7)** 🟨 **Medium (8-14)** 🟥 **High (15-25)**

## Evaluate solutions

Selecting the most appropriate solution to a risk involves evaluating the costs of implementing the action against the benefits derived from it.

### Proposed solutions to address the risks:

- accept the risk – 'do nothing' approach
- abandon the planned project completely
- remove the risk entirely by amending the project, such as collecting anonymised information only
- remove an aspect of the risk – thereby reducing its possible impact
- employ safeguards to reduce the likelihood of an event occurring; for instance security measures such as encryption
- employ control measures to reduce the likelihood of an event occurring, such as controlled access to information to address security concerns.

## Privacy risk register

A privacy risk register can be used by project management to record information about identified privacy risks, analysis of risk severity, and evaluation and management of solutions to address the risk.

### A privacy risk register should:

- describe each risk identified in Stage 2
- assess the likelihood and impact of the risk occurring using a risk matrix, taking into account the potential adverse effects on individuals and the service provider, and note any legal implications. For example fines, reputation damage, loss of trust with the service user
- summarise the proposed solutions to reduce or eliminate the likelihood and or impact of the risk occurring
- identify the result – has the risk been minimised, mitigated or accepted?
- justify the solution employed, balancing project aims with the likely implications for the public or individuals involved.

# Stage 4 - Produce the PIA report

Stage 4 involves the development of a report which details the proposed project, the steps that were undertaken as part of the PIA process and any subsequent recommendations. It should therefore contain the outputs of Stages 1, 2 and 3 of the PIA process. This is a crucial element of the GDPR's requirement for evidence-based compliance.

Service providers are not legally obliged to publish PIA reports, however public organisations may benefit from doing so to build a culture of accountability and transparency, and inspire public confidence in the service provider's handling of personal health information. A summary document might suffice for publication, especially if the full PIA report contains sensitive findings such as security risks.

## Who should be involved?

The PIA report should be quality assured and approved by senior management. This increases accountability for the handling and protecting of personal health information.

A PIA report should focus on the needs and rights of individuals whose personal health information is collected, used or disclosed. The report should be easily understood by the public and written in a clear, coherent manner so that the PIA is communicated effectively. The National Adult Literacy Agency (NALA) has useful resources to aid writing in plain English at www.nala.ie.

## Proposed structure of the PIA report

The structure and format of the report will vary depending on the project and its particular specification.

### At a minimum, the PIA report should include:

an overview of the PIA process undertaken, documenting each stage to ensure compliance with the GDPR including:

- **Stage 1**
  - a copy of the threshold assessment
- **Stage 2**
  - project and organisation description, with an emphasis on the scope and information flows of the project
- **Stage 3**
  - risk analysis; description and rating of each risk
  - solutions to safeguard privacy, with rationale for each solution recorded
  - outline of any remaining risks that could not be resolved, consultation with the Data Protection Commissioner and a business case outlining their justification, if required
  - details of any stakeholder consultation; with individuals or the general public.

# Stage 5 - Incorporate the PIA outcomes into the project plan

In Stage 5, an action plan is developed and, if required, the PIA is reviewed and updated. As the objective of a PIA is to influence the design of a project to ensure the privacy of personal health information is respected and enforced; one of the most important steps of the PIA is addressing the recommendations in order to ensure that improvements are made. Therefore, the project plan should be modified following the outcomes of the PIA. A project action plan keeps track of recommendations made through the PIA process and outlines those responsible for incorporating changes into the project.

## Who should be involved?

The service provider, as the legal Data Controller, is ultimately responsible for the project risks. The ongoing management of the project's privacy risks should be incorporated into the service provider's overall risk management strategy.

If the PIA has been conducted by an external expert, it is imperative for business continuity that a full handover is conducted with the relevant person so that the PIA cycle can continue. If the PIA has been conducted within the organisation, then the ownership of reviewing the PIA should be outlined.

## PIA action plan

An action plan should be developed to manage the implementation of the PIA recommendations into the project. It is important to ensure that actions are carried out prior to the project going live.

| Recommended action(s) | Person responsible | Date solution to be completed | Status |
|---|---|---|---|
| *Amendment to be made to the project following the PIA process* | *Identify the person responsible for implementing the action* | *Deadline for action to be implemented prior to data collection begins* | *Indicate the status of the action – for example, ongoing, complete* |
| | | | |
| | | | |
| | | | |

## Review of the PIA

A PIA should be regarded as an ongoing process that does not end with the preparation of the PIA report.

**The PIA should be treated as a 'live document' and revisited:**

- as the project progresses
- if the organisational or societal context for the project changes significantly
- if the aims of the project change during the project lifecycle.

**If the changes to the project create new privacy implications:**

- the threshold assessment (Stage 1) may need to be revisited to ensure that the PIA is still appropriate
- a new PIA may need to be undertaken if the changes are substantial and result in significant privacy risks that were not considered in the original PIA.

## Additional resources available on www.hiqa.ie

- Guidance on Privacy Impact Assessment in health and social care: Version 2.0
- International review of Privacy Impact Assessments: Version 2.0
- Guidance on information governance for health and social care services in Ireland
- What you should know about information governance: A guide for health and social care staff
- Information management standards for national health and social care data collections
- Five quality improvement tools for national data collections
- What you should know about data quality: A guide for health and social care staff
- Guiding Principles for national health and social care data collections
- Guidance on developing key performance indicators and minimum data sets to monitor healthcare quality
- National standard demographic dataset and guidance for use in health and social care settings in Ireland.
- Guidance on messaging standards in Ireland
- Guidance on classification and terminology standards for Ireland.

Health
Information
and Quality
Authority

An tÚdarás Um Fhaisnéis
agus Cáilíocht Sláinte

Published by the Health
Information and Quality Authority.

**For further information please contact:**

Health Information and Quality Authority
Dublin Regional Office
George's Court
George's Lane
Smithfield
Dublin 7
D07 E98Y

Phone: +353 (0) 1 814 7400
Email: info@hiqa.ie
Web: www.hiqa.ie