Health Information and Quality Authority

An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

Health Information and Standards

Guidance on Privacy Impact Assessment in health and social care

Version 2.0

October 2017

Safer Better Care

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.

HIQA aims to safeguard people and improve the safety and quality of health and social care services across its full range of functions.

HIQA's mandate to date extends across a specified range of public, private and voluntary sector services. Reporting to the Minister for Health and engaging with the Minister for Children and Youth Affairs, HIQA has statutory responsibility for:

- **Setting Standards for Health and Social Services —** Developing person-centred standards, based on evidence and best international practice, for health and social care services in Ireland.
- **Regulation —** Registering and inspecting designated centres.
- **Monitoring Children's Services —** Monitoring and inspecting children's social services.
- **Monitoring Healthcare Safety and Quality —** Monitoring the safety and quality of health services and investigating as necessary serious concerns about the health and welfare of people who use these services.
- **Health Technology Assessment —** Providing advice that enables the best outcome for people who use our health service and the best use of resources by evaluating the clinical effectiveness and cost-effectiveness of drugs, equipment, diagnostic techniques and health promotion and protection activities.
- **Health Information —** Advising on the efficient and secure collection and sharing of health information, setting standards, evaluating information resources and publishing information about the delivery and performance of Ireland's health and social care services.

Overview of the Health Information function of HIQA

Health is information-intensive, generating huge volumes of data every day. It is estimated that a significant amount of the total health budget may be spent one way or another on handling information, collecting it, looking for it, and storing it. It is therefore necessary that information is managed in the most effective way possible in order to ensure a high-quality, safe service.

Safe, reliable healthcare depends on access to, and the use of, information that is accurate, valid, reliable, timely, relevant, legible and complete. For example, when giving a patient a drug, a nurse needs to be sure that they are administering the appropriate dose of the correct drug to the right patient and that the patient is not allergic to it. Similarly, lack of up-to-date information can lead to the unnecessary duplication of tests — if critical diagnostic results are missing or overlooked, tests have to be repeated unnecessarily and, at best, appropriate treatment is delayed or at worst not given.

In addition, health information has a key role to play in healthcare planning decisions – where to locate a new service, whether or not to introduce a new national screening programme and decisions on best value for money in health and social care provision.

Under section (8)(1)(k) of the Health Act 2007, HIQA has responsibility for setting standards for all aspects of health information and monitoring compliance with those standards. In addition, HIQA is charged with evaluating the quality of the information available on health and social care — section (8)(1)(i) — and making recommendations in relation to improving the quality and filling in gaps where information is needed but is not currently available [section (8)(1)(j)].[(1)]

Information and communications technology (ICT) has a critical role to play in ensuring that information to drive quality and safety in health and social care settings is available when and where it is required. For example, it can generate alerts in the event that a patient is prescribed medication to which they are allergic. It can support a much faster, more reliable and safer referral system between the general practitioner (GP) and hospitals.

Although there are a number of examples of good practice, the current ICT infrastructure in health and social care services in Ireland is highly fragmented with major gaps and silos of information. This results in individuals being asked to provide the same information on multiple occasions.

Information can be lost, documentation is poor, and there is over-reliance on memory. Equally those responsible for planning our services experience great

difficulty in bringing together information in order to make informed decisions. Variability in practice leads to variability in outcomes and cost of care. Furthermore, we are all being encouraged to take more responsibility for our own health and wellbeing, yet it can be very difficult to find consistent, understandable and trustworthy information on which to base our decisions.

As a result of these deficiencies, there is a clear and pressing need to develop a coherent and integrated approach to health information, based on standards and international best practice. A robust health information environment will allow all stakeholders — patients and service users, health professionals, policy makers and the general public — to make choices or decisions based on the best available information. This is a fundamental requirement for a highly reliable healthcare system. Through its health information function, HIQA is addressing these issues and working to ensure that high-quality health and social care information is available to support the delivery, planning and monitoring of services.

This updated version of the *Guidance on Privacy Impact Assessment in health and social care* will benefit service providers by informing and increasing awareness on the use of privacy impact assessments in health and social care settings to demonstrate transparency and compliance with privacy and data protection legislation.

Table of Contents

Version Control

This table shows the version history for the *Guidance on Privacy Impact Assessment in health and social care* document.

Publication date	Version	Change
December 2010	1.0	First publication
October 2017	2.0	Guidance fully revised to reflect legislative changes

Document outline

Part 1 of this document introduces the concept of privacy and the importance of information in providing high-quality, safe health and social care services. It provides background information on current legislation and policy in this area and indicates the role of the Health Information and Quality Authority (HIQA) in this regard. It details the role of Privacy Impact Assessments (PIAs) in protecting privacy, their benefits and limitations.

Part 2 of this document outlines the step-by-step process in undertaking a PIA. It identifies important factors to be taken into consideration and provides sample questions on areas to be addressed in identifying real or potential risks to privacy.

Acknowledgements

HIQA would like to sincerely thank all those who participated in informing this updated version of the *Guidance on Privacy Impact Assessment in health and social care* through advising on the international background review and participating in the targeted consultation.

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 guidance. A full glossary of terms is provided in Appendix 1.

General Data Protection Regulation:
The General Data Protection Regulation (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):
The PIA process is 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. A PIA is best undertaken at the beginning of a project before any significant investment has been made, when the outcome of the PIA can influence the design of the project. A PIA should also be carried out when a change to a project is proposed. Throughout the project, the PIA will need to be revisited, reviewed and updated when necessary to incorporate changes to the project as it progresses.
The term 'Data Protection Impact Assessment (DPIA)' is used in the GDPR (see section 1.5).

Service provider:
This term is used in this guidance 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'*.

Service user:
This term is used in this guidance to describe individuals whose personal health information is potentially being collected, used and disclosed by a service provider. For example:

- people who use health and social care services as patients
- carers, parents and guardians
- organisations and communities of interest that represent the interests of people who use health and social care services
- members of the public and communities who are potential users of health services and social care interventions.

Data protection legislation, including the GDPR, refers to the legal term 'Data Subject'*.

*See glossary in Appendix 1 for full definition of terms.

Data Protection Officer:
A Data Protection Officer is a designated person appointed by an organisation to advise on data protection practices. Under the GDPR, a Data Protection Officer is required for public bodies if the organisation performs large-scale processing of sensitive data or performs extensive monitoring of data subjects.

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.

Processing:
The processing of personal health information means performing any operation or set of operations on the information or data, whether or not by automatic means, including:

(a) obtaining, recording or keeping the information
(b) collecting, organising, storing, altering or adapting the information
(c) retrieving, consulting, sharing or using the information
(d) disclosing the information or data by transmitting, disseminating or otherwise making it available, or
(e) aligning, combining, matching, blocking, erasing or destroying the information.

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.

The definition of personal health information has been broadened under the GDPR to include: an individual identifier, genetic data, biological sample data, in vitro diagnostic test, and biometric data such as imaging.

Personal health information relates to an individual who is or can be identified. Pseudo-anonymised data requires the same privacy provisions as identifiable information if there is a chance that an individual could be identified either from:

- the data itself
- the data combined with other information freely available to the 'Data Controller'.

Part 1: The role of Privacy Impact Assessments (PIAs) in assessing risks to privacy

1. Introduction

Information is a vital resource in the delivery of high-quality, safe health and social care services. Service providers collect, use, store and disclose personal health information to provide care. This can present a risk to the privacy and confidentiality of service users as increasing amounts of personal health information are processed. However, there is a need to strike an appropriate balance between using personal health information to provide appropriate and safe care, while continuing to protect individuals' rights to privacy and confidentiality.(2) Privacy Impact Assessments (PIAs) form a fundamental part of information governance in assuring that individuals' rights to privacy and confidentiality are appropriately protected. PIAs are used across all sectors but are particularly important in the context of personal health information, as this is regarded as being sensitive information and merits higher protection under privacy legislation.

The completion of a PIA enables all providers of health and social care services to review management and practices in the handling of personal health information with a view to achieving compliance with legislation and best practice. Undertaking a PIA at the earliest possible stage of a project helps identify potential privacy issues and allows time for solutions and mitigations to be put in place prior to the project 'going live'. This increases awareness among professionals and creates a culture where maintaining personal health information privacy is a priority.

1.1 Background

The primary mandate of the Health Information and Quality Authority (HIQA) is to ensure quality and safety in health and social care in Ireland. In relation to HIQA's health information function this includes ensuring that individuals' rights are appropriately protected and that the privacy, confidentiality and security of their personal health information is assured.

The *National Standards for Safer Better Healthcare*, published in 2012, describe a vision for quality and safety in healthcare which includes the use of accurate and timely information to promote effectiveness and drive improvements.(3) 'Use of information' is one of the eight themes of the standards, highlighting the importance of actively using information as a resource for planning, delivering, monitoring, managing and improving care.

In January 2017, HIQA published *Information management standards for national health and social care data collections* in Ireland. These standards complement the *National Standards for Safer Better Healthcare* and collectively provide a roadmap to improve the quality of health information and data, to drive improvements in national health information and ultimately contribute to the delivery of safe and

reliable health and social care.[4] Privacy Impact Assessments are outlined in the standards as a useful tool to ensure that individuals' rights are appropriately protected:

> Standard 1, feature 1.3: 'Development and use of privacy impact assessments (PIAs) to assure that data subjects' rights to privacy, confidentiality and security are appropriately protected'.

HIQA previously published *Guidance on Privacy Impact Assessment in Health and Social Care* in 2010[5] and *Guidance on information governance for health and social care services in Ireland* in 2012.[6] In light of the forthcoming General Data Protection Regulation (GDPR) in May 2018, HIQA has revised the *Guidance on Privacy Impact Assessment in health and social care* to reflect the legislative changes.

1.2 Purpose of this guidance

This document has been developed as a resource to support service providers:

- to protect the privacy rights of individuals who use their services
- to strengthen governance arrangements around personal health information.

The guidance outlines a step-by-step process for undertaking a PIA and the important factors to be considered at each stage of the process.

1.3 Methodology

The guidance update was developed in line with HIQA's guidance development process. This was informed by a detailed background review of international best practice, which is published on the HIQA website. A summary of international evidence is outlined in Appendix 2. The development of this PIA guidance has drawn strongly from international best practice in other jurisdictions. A targeted consultation was undertaken with experts and key stakeholders to provide feedback on the development of the guidance. Following the targeted consultation, HIQA analysed the feedback and revised the guidance as appropriate.

1.4 Privacy

1.4.1 What is privacy and why is it important?

Privacy can be defined simply as the right to be left alone.[7] In terms of personal health information, privacy can be described as the right of individuals to keep their information confidential.[8] Health information is considered to be one of the most sensitive forms of information. Providers of health and social care services 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. Personal health information is a valuable commodity and it is vital that it is treated as such.

1.4.2 Service provider responsibilities in relation to privacy

Privacy is a human right enshrined in both Irish and European legislation. Service providers, as legal Data Controllers, 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 individual privacy and providing safe, effective care. The human right to privacy is legislated under:

- The Irish Constitution, Article 40.3.1: 'The State guarantees in its laws to respect, and, far as practicable, by its laws to defend and vindicate the personal rights of the citizen'[9]
- The European Convention of Human Rights, Article 8: 'Right to respect for private and family life', as currently enshrined in Irish legislation under the European Convention on Human Rights Act 2003.[10,11]

1.4.3 Individuals' rights in relation to privacy

Each individual accessing health and social care has specific rights in relation to their privacy. Data protection legislation also ensures that the right to privacy is protected by those who collect, use and disclose personal 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.[12]

1.4.4 Data protection legislation - GDPR

The General Data Protection Regulation (GDPR) comes into effect on 25 May 2018 and will replace Ireland's Data Protection Acts[13] and the existing EU Data Protection Directive.[14]† 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, with specific requirements for transparency, more extensive rights for data subjects and stronger penalties for non-compliance.[15] Some principles are new such as 'data protection by design' and 'data protection by default'. In practice, this means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy.[15] Some of the key requirements under the GDPR relevant to this guidance are the following:[15,16]

- Data Protection Impact Assessment (DPIA):
  There is a mandatory obligation to conduct a DPIA where a processing is 'likely to result in a high risk' to the rights and freedoms of data subjects. Data concerning health is categorised as 'sensitive data' requiring a DPIA, which includes genetic, biometric or unique identifier data. A DPIA is required per 'processing activity'; however, this document uses the term 'project' to describe the processing of personal health information.
- Data Protection Officer:
  There is a mandatory obligation to appoint a, suitably qualified and experienced, Data Protection Officer within an organisation for;
  - public bodies
  - if the organisation performs large-scale processing of sensitive data
  - if the organisation performs extensive monitoring of data subjects.

†The General Scheme of the Health Information and Patient Safety (HIPS) Bill was published on 10 November 2015; however at the time of publishing this guidance the Bill had yet to be enacted. This Bill was drafted to safeguard the privacy of individuals to ensure that there can be public confidence in prescribed health information resources.

The Data Protection Officer must be consulted and should oversee the progress of the DPIA.

- Data subjects:
  Data Controllers are obliged to seek the views of data subjects or their representatives where appropriate on the privacy risks identified in the DPIA and the ways to address them.

- Supervisory authority:
  The supervisory authority is responsible for enforcing the obligations on Data Controllers holding and processing personal health information. In the Irish context, this role is undertaken by the Office of the Data Protection Commissioner. The supervisory authority must be consulted if the DPIA does not identify mitigating safeguards against residual risks.

- Data Controller:
  Data Controllers are obliged to carry out a DPIA to protect the privacy of the individuals whose personal health information they collect. Data Controllers are fully accountable for the methodological choices of a DPIA and appropriately documenting it.

1.5 Privacy Impact Assessment (PIA)

The Office of the Data Protection Commissioner in Ireland has developed Guidance on Data Protection Impact Assessments (DPIA) in the context of the GDPR.[17] The term 'Privacy Impact Assessment' (PIA) is often used interchangeably with the term 'Data Protection Impact Assessment' (DPIA).[18] However, data protection is only one aspect of privacy.[19] A PIA ensures that privacy is considered as a human right, as well as ensuring compliance with the GDPR obligation of undertaking a DPIA.[19] 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.

Service providers are obliged to conduct a PIA to protect the privacy of the individuals whose personal health information they collect. The primary objective of a PIA is to weigh up any negative privacy impacts of a project against the benefits offered to the public. 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. Service providers are fully accountable for carrying out a PIA and documenting it appropriately.

The PIA process begins at the planning stage of any new or significantly amended programme, initiative, system or project that involves the collection, use or disclosure of personal health information. PIAs serve as an 'early warning system' for the organisation, detecting potential privacy problems and identifying precautions to be undertaken at the earliest possible stage.

1.5.1 Benefits of PIA

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.

The benefits of undertaking a PIA include the following:

- Ensuring the privacy rights of individuals are protected.
- Ensuring and demonstrating that the organisation complies with legislation; service providers who undertake PIAs appropriately demonstrate that the privacy of individuals is a priority for the organisation, and show commitment to putting the rights of the individual first through the proper handling of personal health information. This helps to build trust between the service provider and the individual.
- Enabling the service provider to incorporate 'data protection by design'[‡] into new projects.
- Reducing operation costs by conducting a PIA in the early stages of planning a project, optimising information flows within a project and eliminating unnecessary data collection and or processing.
- Reducing the cost and disruption of data protection safeguards by integrating them into project design at an early stage, as potential privacy risks or issues are much simpler to resolve prior to any substantial investment.
- Providing evidence through the PIA report that the service provider acted appropriately in attempting to prevent the occurrence of a privacy risk or breach. This can help to reduce or even eliminate any negative publicity and loss of reputation in the event of an unavoidable occurrence.

[‡] 'Data Protection by design' means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy.

1.5.2 Considerations of PIA

A PIA in its own right may not highlight all privacy risks or issues associated with a project. It is important to understand that a PIA is a tool used to assess privacy risks and so is very dependent on service providers having the correct processes in place to carry out the PIA. These include:

- identification of the appropriate stakeholders for the assessment
- selection of those with the necessary knowledge and skills to carry out the PIA
- involvement of senior managers to ensure the implementation of any recommendations made as a result of the PIA.

It is essential that the PIA is reviewed and updated regularly to reflect any changes to the direction of the project. This ensures that all identifiable privacy risks are addressed. A PIA is intended to be an integral part of the project management process for new projects or significant amendments to current projects.

Issues may arise in projects that are beyond the scope of this guidance or that require more detailed consideration and analysis. Service providers should continue to use their good judgment, in parallel with this guidance, for projects undertaken that involve personal health information. This guidance does not guarantee compliance with the provisions in privacy or data protection legislation, or any other legislation governing the collection, use or disclosure of personal information. Advice on compliance with legislation can be sought from the designated Data Protection Officer of the organisation or independent legal advisors.

Part 2: The Privacy Impact Assessment (PIA) Process

2. Introduction to the PIA Process

This guidance document provides step-by-step assistance through each stage of the PIA process and identifies the key areas for consideration. The sections that follow offer practical advice on how to undertake a PIA. A PIA threshold assessment checklist has been provided in Appendix 4.

2.1. Who should conduct a PIA?

The PIA process should be undertaken by the service provider and carried out by the person or people identified as having the appropriate expertise and knowledge of the project in question. As such, it should generally be undertaken by the project team. The designated Data Protection Officer of the organisation should be consulted and should monitor the progress of the PIA process. The views of individuals or their representatives should be consulted as appropriate. Additionally, if a third party organisation is processing the data on behalf of the service provider, the third party should assist with the PIA and provide any necessary information required. If the service provider does not identify sufficient safeguards or control measures to mitigate residual high risks, the Office of the Data Protection Commissioner should be consulted. The service provider is responsible for the completion of the PIA and for implementing any changes to the project plan following recommendations for privacy enhancement or risk mitigation that arises from the PIA.

PIAs should be reviewed, quality assured, approved and signed off at senior management level. The Data Controller (service provider) is ultimately responsible for ensuring that the PIA is carried out appropriately. For example, the Director General of the Health Service Executive (HSE) was responsible for the PIA conducted on the Individual Health Identifier.[20] Similarly, HIQA's Chief Executive Officer was responsible for the National Patient Experience Survey Programme's PIA.[21]

2.2. When should a PIA be undertaken?

A PIA should be undertaken prior to the processing of any personal health information. A PIA is most beneficial when it is conducted in the early stages of a project – ideally at the planning stage. If it is conducted early, the outcome of the PIA can significantly influence the development of a process before any substantial investment has been made. On the other hand, if a PIA is conducted too early in the process the results will be vague as there may not be enough information available about the project, its scope and proposed information flows to properly consider the privacy implications. It is recommended that the PIA should be a 'live document' which can be revised as the project develops or changes throughout the project

lifecycle. The PIA process should be undertaken when a project proposal is in place but before any significant progress or investment has been made.

The findings and recommendations of the PIA should influence the final detail and design of the project. Conducting PIAs should be embedded as part of the project management framework so that the management of privacy risk is an ongoing process. The PIA should evolve in line with changes to the project.

Prior to personal health information being processed:

- a PIA should be undertaken
- recommendations to the project design should be implemented
- the PIA should be revised and reviewed at the end of the project's planning stages to ensure that the PIA is still relevant and has considered all privacy risks.

2.3. Stakeholder consultation

The GDPR states that the views of stakeholders should be sought, and documented, when undertaking a PIA.[15] Consultation with key stakeholders is an important element of the PIA process. It 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, with both internal and external stakeholders, into each stage of the PIA process. Many stakeholder consultation models exist, for example; interviews, surveys, focus groups, and workshops. Careful consideration should be given to which model would be appropriate to gather the information required. For the consultation process to be successful, all stakeholders should be sufficiently informed of the project, should be given the opportunity to express their views and raise any concerns, and they should be assured that their perspectives will be taken into account in the design of the project.[22]

Stakeholders include those who are interested in, or may be affected by, the project being considered. It may be useful to identify the key stakeholders by creating a list during the beginning stages of the PIA process which can be updated as the project progresses.

2.3.1 Internal consultation

Internal consultation with colleagues is an important part of any PIA. Internal consultation can include informal or formal discussions via email or more structured meetings. Internal consultation with those who will be working on the project or carrying out the procedures can help to identify and mitigate risks that may otherwise go undocumented. Examples of internal stakeholders include:[23]

- project team
- designated Data Protection Officer of the organisation
- IT staff
- records management personnel
- communications team
- senior management.

2.3.2 External consultation

External consultation means seeking the views of the people who will be affected by the project, such as service users or their representatives. External consultation helps providers understand the concerns of the individuals who may be affected by the project, and also improves transparency by making people aware of how information about them is being used. Feedback from additional parties may be useful, such as third party organisations, industry experts and academics. External consultation generally uses a more formalised process which may include focus groups, user groups, workshops, public consultations and stakeholder interviews. Effective external consultations should follow these principles:[23]

- Timely – at the right stage and allow sufficient time for responses.
- Clear and proportionate – in scope and focused.
- Reach and representative – ensure that those likely to be affected have a voice.
- Ask open, transparent, objective questions and present realistic options.
- Feedback – ensure that those participating get feedback at the end of the process.

2.4 The PIA Process

The PIA process involves the evaluation of privacy implications of projects and relevant legislative compliance. Where potential privacy risks exist, ways to avoid or mitigate these risks are identified. There are five stages in the PIA process:

Stage 1: Threshold assessment
This stage requires the project team to answer a number of questions about the project to determine if it presents any potential privacy risks. The answers to the questions determine if it is necessary to proceed with the PIA process.

Stage 2: Identify the privacy risks
This stage involves identifying the privacy risks through exploring the privacy management, scope, objectives, systematic description of the processing, mapping the information flows and security arrangements of the project.

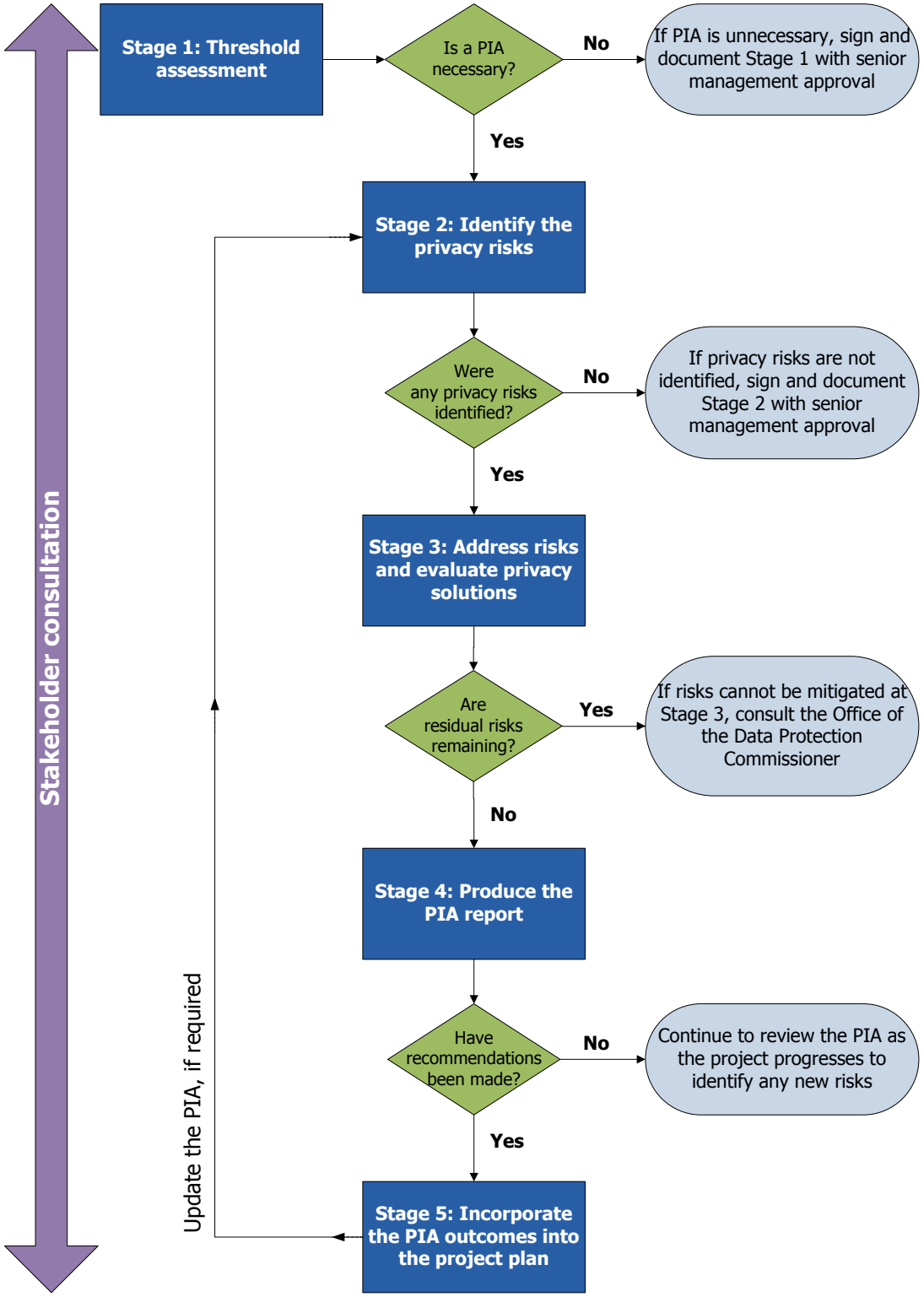
Stage 3: Address privacy risks and evaluate solutions
This stage deals with addressing the privacy risks identified in Stage 2. This is achieved firstly through assessing the risks and then analysing safeguards or control measures to avoid or mitigate the potential risk.

Stage 4: Produce the PIA report
The output of the PIA process is a PIA report containing the details of each of previous three stages, where appropriate. The PIA report should be publicly available, in full or summary form, as best practice in transparency.

Stage 5: Incorporate the PIA outcomes into the project plan
A PIA should be regarded as an ongoing process that does not end with the preparation of the PIA report. It is important that action is taken in order to ensure that the recommendations included in the report are carried out. PIA outcomes should be integrated into the project plan. The PIA should be monitored and should be a 'live' document.

Figure 1: The five stages of the PIA process

The figure illustrates the generic iterative PIA process. In practice it is likely that each of the stages will be revisited multiple times before the PIA can be completed. Each stage of the PIA process must be documented to ensure compliance with the GDPR.



3. Threshold assessment (Stage 1)

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 the service provider's project management processes to ensure that privacy is routinely considered at the beginning of a project. This applies not only to new projects but also to proposals to amend existing information systems, sources or processes.

The threshold assessment should be carried out by the project team. 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. The questions seek to ascertain, for example, whether the information will be used for research or statistics. A template for a PIA threshold assessment is available in Appendix 4.

Sample questions to be asked as part of the threshold assessment are outlined below.

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?

3.1. Next steps

The threshold assessment results in two possible outcomes for the project team, that is to say, either to proceed or not with the PIA.

- 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 the threshold assessment is that a PIA is required, consult the designated Data Protection Officer of the organisation for advice. It is a requirement under the GDPR that the Data Protection Officer is consulted and kept informed of the PIA's progress.[(15)] Before undertaking the PIA, consider the team required, set out the terms of reference, consider the benefits of conducting the PIA internally or getting an external consultant.

Each stage of the PIA process must be documented to ensure compliance with the GDPR.[(15)]

4. Identify the privacy risks (Stage 2)

If it is deemed necessary to continue with the PIA following the threshold assessment, the process proceeds to Stage 2. This stage involves identifying potential privacy risks by examining how the service provider manages privacy and exploring the project's information flows with regard to individuals' fundamental right to privacy. 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.

Stage 2 of the PIA requires the service provider to explore and document the following:

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

Each of these sections is discussed in turn below.

4.1. Privacy management arrangements of the service provider

Privacy management arrangements relates to how the service provider manages the privacy of personal health information in relation to the current project. The privacy arrangements of the service provider need to be considered to put the project, and any potential risks to individuals' fundamental right to privacy, into context.

It explores information governance management such as; staff awareness of data protection and confidentiality, education and training of staff on data protection and confidentiality, and accountability for the handling of personal health information (see section 4.4 on stakeholder consultation).

Examples of questions to be asked in relation to the privacy management arrangements of the service provider are outlined in the box below.

In light of the current project, key considerations of the service providers privacy:

- Is the service provider the legal Data Controller for all personal health information within the scope of the project?
- Are third party organisations involved and are there service-level agreements documented outlining their roles and responsibilities?

- Who is the designated Data Protection Officer of the organisation?
- Is there a privacy policy in place outlining the safeguards employed to protect individuals' privacy and confidentiality?
- Is there a statement of information practices in place which sets out the types of information collected, where it is collected, how it is used, if it is shared and how individuals can access information held about them?
- Is there a records management policy in place which includes a retention and destruction schedule? This should outline how long particular types of personal health information are held for and the process around the secure disposal of both paper and electronic records.
- Are project members who have access to personal health information provided with training related to implementing the privacy policy? If so, describe the training and outline the training schedule in place.
- Are administrative, technical and physical safeguards in place to protect personal health information against theft, loss, unauthorised use or disclosure and unauthorised copying, modification or disposal?
- Is the privacy breach management action plan up to date and fully implemented?

4.2. Description of the project

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 privacy risks in context. It is imperative to explore the scope of the project to determine how far-reaching its impact is likely to be. This section looks at indicators such as the proportion of the population upon which the project impacts and the effects the project is likely to have on the individuals involved. In the case of a national project, this may be the general population. It can also be the population of individuals of a particular service provider that may be affected by the project. 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?
- 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?

4.3. Mapping information flows

Following a description of the project's overall nature and scope, the next step is to map the project's information flows. This stage should consider the privacy of information in terms of collection, use, quality, security, disclosure, access and correction, retention, storage and disposal. The analysis should be sufficiently detailed to identify privacy risks. In order to effectively map the information flows, it will also be necessary to communicate with other staff and key project stakeholders (see section 4.4).

This section is designed to help produce a clear picture of the information flows within the envisaged project. Understanding the life cycle of information from collection to disposal can help determine where risks to privacy could occur.

Detailed mapping of the information flows should examine the following areas:

- What personal health information will be collected?
- Where will the information be sourced?
- How will it 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?

As is the case for the other stages, these questions serve to focus the areas for consideration, and are not intended to be exhaustive. Service providers should answer each of these questions, and others as appropriate, in as much detail as possible, highlighting any potential privacy risks in relation to each of the answers provided. Sample questions to identify potential privacy risks as part of the information mapping stage are listed below.

The following sample questions will aid in identifying potential privacy risks.

Collection of the information:

- What information is to be collected?
- Where is the information being collected?
- How is the information to be collected?
- Why is the information being collected? Justify the necessity of the information in relation to the project.
- How often the personal information is to be collected?
- Can the project proceed using anonymous or de-identified information?

Uses of the information:

- How will information be used? Identify and describe all the uses of the personal health information and how these uses relate to the purpose of the project.
- When will the information be processed? (e.g. on a systematic basis, only in certain cases, during a limited period of time, etc)
- How will the information be handled? Describe the processes.

Secondary use of information:

- Is it a possibility that the information will be linked, matched or cross-referenced with an existing or proposed project?
- Is consent required for secondary use?
- Is the use of information related to the purpose of the collection?
- Can an individual refuse consent for secondary purposes and still be involved in the project?

Information quality:

- What are the consequences for individuals if the personal information is not accurate or up-to-date?
- What are the processes that ensure only relevant, up-to-date and complete information will be disclosed?

Information security:

- What security measures will be taken to protect the information from loss, unauthorised access, use, modification, disclosure or other misuse? Include information on how data is transferred from sites or systems.
- How will personal information be protected if it is to be managed by someone else?
- Who has access to the information? Who will authorise access to the information? Outline the identity of the service provider, the third party processor etc. Have the roles and responsibilities of each been appropriately documented, for example in service contracts?

- What systems are in place to prevent or detect misuse or inappropriate access?

Access and correction:

- What arrangements are in place to allow individuals to access information that is held about them? Include any costs to the individual.
- How can an individual correct any factual inaccuracies in personal health information held about them?
- How will decisions be made about requests from individuals for access to or correction of their information?

Disclosure of information:

- To whom, how and why will personal information will be disclosed?
- Will the information be shared outside of the purposes of this project?
- What safeguards or precautions are in place to limit inappropriate access, use and disclosure of the information?

Retention, storage and disposal:

- What are the retention and destruction practices to be employed in the project?
- When will personal information be de-identified or destroyed?
- How will this be done securely?
- Where will the data be processed and stored? Include information on storage location and data transfers.
- What is the data retention period?

4.4. Next steps

Having completed Stage 2 of the PIA, the next steps to be taken will depend on whether or not the service provider has identified any potential privacy risks with the new processing procedure or existing issues with systems currently in place.

- If privacy risks are not identified in Stage 2, the process should be documented, signed by the project team and approved by senior management as appropriate.
- If privacy risks have been identified at Stage 2, the next stage of the PIA - Stage 3 - involves a full assessment of the areas that present risks and an analysis of how best to mitigate or avoid them.

Each stage of the PIA process must be documented to ensure compliance with the GDPR.[(15)]

5. Address privacy risks and evaluate solutions (Stage 3)

The purpose of this stage of the PIA process is to assess, analyse and address the types of privacy risks to individuals' personal health information identified at Stage 2. Once the risks have been identified as part of Stage 2 of the PIA process, the risks can be assessed and combined or grouped as appropriate. For example, if more than one risk with regard to sharing personal health information is highlighted, these can be grouped, analysed and addressed together.

The steps involved in Stage 3 are:

- analyse privacy risks
- evaluate privacy solutions
- stakeholder consultation.

For this stage of the PIA process, consultation of service users or their representatives should be conducted. Through consultation, fresh insights on the perceptions of the impact of privacy risks can be gathered, and potential solutions can be suggested by the individuals to reduce or mitigate the risks.

If there is a residual or remaining 'high risk' which cannot be mitigated at Stage 3, the PIA lead must consult the Office of the Data Protection Commissioner for advice and the project team should decide whether or not it is acceptable to continue with the project. If a decision is made to proceed with the 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.

Stage 3 of the PIA process should be reviewed and approved by a member of senior management in the organisation.

5.1. Analyse privacy risks

Risk analysis is about developing an understanding of privacy risks to the rights and freedoms of individuals. It has been defined as a systematic process to understand the nature of risk and to deduce the level of risk involved. In analysing the risks it is necessary to determine the impact and the likelihood of a particular event occurring, thereby determining the level of risk. Analysing risks is an ongoing process – it should be repeated whenever there is a change in the circumstances that affect a risk. In the case of health information projects, service providers should consider the likelihood and impacts of the event occurring, both to individuals and to the service. This will enable service providers to rate the risk accordingly.

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?

5.1.1 Risk matrix

One approach to analysing risks is through the use of a risk matrix – a useful tool for ranking and displaying risks by defining ranges for impacts and likelihood. A sample risk matrix is presented in Figure 2. A risk matrix can be used to capture the likelihood of the event occurring and the potential impact it would have. For example, if it is very likely that information collected for one project would be used for secondary purposes without the consent of the individuals involved, this would be recorded as a high risk which would impact the progress of the project.

Figure 2: Sample privacy risk matrix structure

	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)**

5.2. Evaluate privacy solutions

Following the analysis of each risk, the next step is to identify ways to mitigate the risk by reducing or eliminating the likelihood of each risk occurring. The positive effects of risk mitigation should always be balanced against how the goals of the project will be affected. Selecting the most appropriate solution to a risk involves evaluating the costs of implementing the action against the benefits derived from it. In each case, the cost of mitigating a risk should be appropriate and proportionate to the value gained in terms of protection of personal health information gains. The

control measure employed should be the option that is effective and the least intrusive into individuals' lives, protecting their right to privacy and ensuring compliance with data protection laws. Every effort should be made to ensure that risks are analysed and privacy solutions are put in place at the earliest possible stage of project planning.

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 adopting 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.

5.2.1 Privacy risk register

Service providers should follow the processes outlined in their risk management policies for this section of the PIA. A privacy risk register can be used by project management to record information about identified privacy risks, analysis of risk severity, the evaluation and management of solutions to address the risk.[17]

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.

The privacy risks can be ranked by risk rating in order to highlight the highest priority risks for those with accountability for the service. The privacy risk register can include a log to track the actions taken to reduce or eliminate risks.

The risk register should be a live document, updated as the project progresses to reflect solutions that have been implemented or new risks that have been identified.

Examples of privacy risks and risk mitigation strategies are outlined below are outlined in the box below.[17,22]

Possible Risks	Potential risk mitigation strategies
Collection of the information: Personal health information will be collected without a clear purpose, which could increase the risk of unauthorised uses and disclosures.	Ensure that the purposes for which personal health information is collected and used are clearly identified and documented and that others in the organisation or agency are aware of these purposes.
Uses of the information: Personal health information being used for purposes not expected by individuals due to failure to effectively explain how their information would be used or due to an evolution in the nature of the project.	Ensure that individuals are fully informed about how their information will be used by publishing a statement of information practices on the service provider's website, on notice boards, and displayed as posters in the organisation. A contact point should be provided for individuals to raise any concerns they may have with the organisation.
Secondary use of information: Individuals may be surprised or upset by a secondary use or disclosure of information, resulting in privacy complaints and or negative publicity.	Undertake further stakeholder consultation to test community expectations about the proposed uses and disclosures of information. Consider whether it is possible to seek consent for secondary uses and disclosures.
Information Quality: Poor quality information may lead to inappropriate decisions that have a negative impact on the individuals concerned.	Check the reliability of tools used to collect or process personal health information. Consider establishing regular checks of tools and procedures for human data processing, such as in-built validation tools for assessing data quality. Identify and document procedures on how often personal health information will be reviewed and

Possible Risks	Potential risk mitigation strategies
	updated.
Information security: Inappropriate access of personal health information internally within the organisation due to a lack of appropriate controls being in place.	Review the physical and or IT security in the organisation or for a particular project team and make appropriate improvements where necessary.
Access and correction: Individuals are not able to easily access information that is held about them and they cannot easily correct factual accuracies.	Identify how access and correction procedures can be made more straightforward. Consider providing individuals with routine access to their personal health information.
Disclosure of information: De-identification of personal health information before disclosure may not prevent re-identification.	Review de-identification procedures to ensure that sufficient details are removed so that the recipient of the information will not be able to re-identify it, or combine it with other information to establish an individual's identity.
Data retention, storage and disposal: Data may be kept longer than required in the absence of appropriate policies.	Put in place strict retention periods, designed to minimise the length of time that personal health information is retained.

These actions, and potentially others, and the consequences for both the individual and the proposed project should be considered and discussed in respect of each risk. The option(s) chosen for each risk, and the justification behind the choices made, should be clearly explained in supporting documentation. Any residual risks should be documented in the service provider's risk register, which should be reviewed, updated and managed on a regular basis by the project team and the senior management. A final review and sign-off of residual risks should be conducted before the project begins data collection.

5.3 Next steps

Stage 3 of the PIA process should be reviewed and approved by a member of senior management from within the organisation. Each stage of the PIA process must be documented to ensure compliance with the GDPR.(15)

Feedback gained and any changes made to a project as a result of stakeholder engagement should be included in the PIA report which is developed at the next step in the process, Stage 4.

6. Produce the PIA report (Stage 4)

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. A completed PIA report highlights and addresses all privacy risks associated with the project and the steps that have been taken to mitigate or avoid them. 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.

The PIA report should be quality assured and approved by senior management from within the organisation. This involves assurance from senior management that the PIA has been conducted appropriately by the appropriate members of staff and that the content of the report is an accurate reflection of the PIA process, the privacy risks of the project and the actions taken to mitigate those risks. This is an important step in increasing accountability for the handling of personal health information and its protection.

6.1 Proposed structure of the PIA report

The focus of a PIA report should be on the needs and rights of individuals whose personal health information is collected, used or disclosed. 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 Office of the Data Protection Commissioner and a business case outlining their justification if required
  - details of any stakeholder consultation; with individuals or the general public.

The report should be easily understood by the general public as the assumed target audience. The completed PIA report should be written as a stand-alone document in

a clear, coherent manner so that the PIA is communicated effectively. The National Adult Literacy Agency (NALA) have useful resources to aid plain English writing of reports - www.nala.ie.[24] The PIA should also be published in an accessible manner and be located in a user-friendly location.

6.2 Benefits of publishing the PIA report

There are a number of benefits to preparing and publishing a PIA report, primarily for the service provider compiling it but which also extend further. Service providers are not legally obliged to publish PIA reports, however public organisations may especially 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. It should be noted that a summary document might suffice for publication, especially if the full PIA report contains sensitive findings such as security risks.

The benefits of publishing the PIA include:

- showing accountability in demonstrating that the PIA process was performed appropriately
- enabling the experience gained and lessons learned throughout the process to be shared both within and outside of the service provider's organisation
- empowering individuals to inform themselves of the way their personal health information is being used and the safeguards that are being put in place to protect it
- demonstrating to the public that their privacy has been given due consideration, thereby improving public trust and confidence in the service provider.

6.3 Next steps

A PIA should be regarded as an ongoing process that does not end with the preparation of the PIA report. Stage 5 ensures that PIA outcomes are incorporated into the project plan.

7. Incorporate the PIA outcomes into the project plan (Stage 5)

In Stage 5, an action plan is developed and, if required, the PIA is reviewed and updated. 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 to the project are made. Therefore, the project plan should be modified following the outcomes of the PIA. A PIA action plan keeps track of recommendations made through the PIA process and those responsible for incorporating changes into the project. The PIA should be monitored and should be a 'live document'.

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.

The steps involved in this stage include:

- developing an action plan
- reviewing and updating the PIA if required.

7.1 PIA action plan

One of the most important steps of the PIA is addressing the recommendations in order to ensure that improvements are made. If privacy risks have been identified, 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.

The action plan should detail:

- the actions that will be taken to mitigate the risks
- the individuals who will be responsible for ensuring that these actions are carried out
- the timeframe for the actions to be carried out.

The ongoing management of privacy risks should be considered and incorporated into the overall risk management strategy of the service provider.

7.2 Review 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 reviewed regularly, incorporated into project management processes and monitored accordingly. As the project progresses, the PIA should be revisited and updated or revised if developments in the design or implementation of the project create new privacy implications that were not previously considered.

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 project aims 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.

8. Conclusion

Privacy Impact Assessments (PIAs) are used across all sectors but are particularly important in protecting personal health information as this is highly sensitive information requiring higher protection. The primary purpose of undertaking a PIA in health and social care is to protect individuals' right to privacy in relation to their personal health information.

This document has been developed as a resource to support service providers in protecting the privacy rights of individuals and strengthening information governance arrangements. The guidance outlines a step-by-step process for undertaking a PIA and the important factors to be considered at each stage of the process.

Having updated this guidance, HIQA will continue to develop and publish additional documents to support improvements in information governance and to protect the rights and interests of health and social care service users.

9. References

1. *The Health Act 2007*. Dublin 2007. Available from: www.irishstatutebook.ie/eli/2007/act/23/enacted/en/pdf.
2. Department of Health and Children. *Quality and Fairness, A Health System for You. Health Strategy*. 2001. Available from: http://www.dohc.ie/publications/quality_and_fairness.html.
3. Health Information and Quality Authority. *National Standards for Safer Better Healthcare*. Dublin 2012. Available from: https://www.hiqa.ie/sites/default/files/2017-01/Safer-Better-Healthcare-Standards.pdf.
4. Health Information and Quality Authority. *Information management standards for national health and social care data collections*. Dublin 2017. Available from: https://www.hiqa.ie/sites/default/files/2017-02/Information-management-standards-for-national-health-and-social-care-data-collections.pdf.
5. Health Information and Quality Authority. *Guidance on Privacy Impact Assessment in Health and Social Care*. 2010. Available from: http://www.hiqa.ie/resource-centre/professionals/privacy-impact-assessments.
6. Health Information and Quality Authority. *Guidance on information governance for health and social care services in Ireland*. 2012. Available from: https://www.hiqa.ie/healthcare/health-information/information-governance.
7. Ireland Office of the Data Protection Commissioner. *Sign Up, Log in, Opt Out: Protecting your Privacy & Controlling your Data*. 2007. Available from: https://www.dataprotection.ie/documents/teens/cspe%20resource%20booklet/Section_1_-_What_is_privacy.pdf.
8. J. and Millar Erickson, S. *Caring for Patients while Respecting their Privacy: Challenges of Maintaining Privacy and Confidentiality*. 2005. Available from: http://www.nursingworld.org/MainMenuCategories/ANAMarketplace/ANAPeriodicals/OJIN/TableofContents/Volume102005/No2May05/tpc27_116017.html.
9. *Bunreacht na hEireann 1937*. Dublin 2012. Available from: https://www.constitution.ie/Documents/Bhunreacht_na_hEireann_web.pdf.
10. European Court of Human Rights 1950. *European Convention on Human Rights* 2010. Available from: http://www.echr.coe.int/Documents/Convention_ENG.pdf.
11. *EUROPEAN CONVENTION ON HUMAN RIGHTS ACT 2003*. 2003. Available from: http://www.irishstatutebook.ie/eli/2003/act/20/enacted/en/pdf.
12. Ireland Data Protection Comissioner. *The Data Protection Rules*. Dublin 2017. Available from: https://www.dataprotection.ie/docs/Data-Protection-Rules/y/21.htm.
13. *Data Protection Act 1988 (Ireland)*. 1988. Available from: http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html
14. EU Directive 95/46/EC. *The Data Protection Directive* 1995. Available from: http://eur-lex.europa.eu/eli/dir/1995/46/oj.
15. *REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. 2016. Available from:

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN.

16. Ireland Data Protection Comissioner. *General Data Protection Regulation*. Available from: https://www.dataprotection.ie/docs/GDPR/1623.htm.

17. Ireland Office of the Data Protection Commissioner. *Data Protection Impact Assessments (DPIA)*. 2017. Available from: http://gdprandyou.ie/data-protection-impact-assessments-dpia/.

18. Article 29 Data Protection Working Party. *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. 2017. Available from: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

19. Trilateral Research. *A Comparative Analysis of Privacy Impact Assessment in Six Countries*. 2013. Available from: http://www.jcer.net/index.php/jcer/article/view/513/393.

20. Ireland Health Service Executive. *Privacy Impact Assessment (PIA) for the Individual Health Identifier: Draft for Public Consultation*. 2016. Available from: http://www.ehealthireland.ie/Library/Document-Library/IHI-Documents/PIA-IHI.pdf.

21. National Patient Experience Survey Programme. *Privacy Impact Assessment (PIA) - Summary Report*. Dublin 2017. Available from: https://www.patientexperience.ie/app/uploads/2017/07/HIQA-NPESP-PIA-Summary-Final-Report-v1-0-July-2017-2.pdf.

22. Office of the Australian Information Commissioner. *Guide to undertaking privacy impact assessments*. 2014. Available from: https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf

23. UK. The Information Commissioner's Office. *Conducting privacy impact assessments code of practice: Data Protection Act* 2014. Available from: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

24. The National Adult Literacy Agency (NALA). *Plain English guidance*. 2017. Available from: https://www.nala.ie/resources/118.

25. Article 29 Data Protection Working Party. *Guidelines on Data Protection Officers (DPOs)*. 2017. Available from: http://ec.europa.eu/newsroom/document.cfm?doc_id=44100.

26. Ministry of Health New Zealand. *Ministry Guidelines on Privacy Impact Assessments (PIA).* 2017.

27. NHS Digital. *Privacy Impact Assessment Report Customer Template* 2017.

28. Treasury Board of Canada Secretariat. *Directive on Privacy Impact Assessment*. 2010. Available from: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308.

29. New Zealand Office of the Privacy Commissioner. *Privacy Impact Assessment Toolkit*. 2015. Available from: https://opcwebsite.cwp.govt.nz/news-and-publications/guidance-resources/privacy-impact-assessment/.

30. European Data Protection Supervisor. *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*. 2017. Available from: https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf.

31. Privacy Impact Assessment Framework. *A Privacy Impact Assessment Framework for data protection and privacy rights*. 2011. Available from: http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf.

10. Appendices

Appendix 1: Glossary

Please note the General Data Protection Regulation (GDPR) has been referenced throughout this glossary.[15]

Term	Description of term
Anonymised information	Anonymised information refers to data or information that cannot be linked to any particular individual, that is to say, the data subject cannot be identified from the information either on its own or in conjunction with additional information (*Recital 26, Article 4[1] of the GDPR*).
Consent	Consent refers to the freely given, specific and informed indication of the data subject's wishes to use their personal health information by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her (*Recital 32, 39, 40, 42, 43; Article 4[11] and Article 7 of the GDPR*).
Data Controller	'Data Controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by European Union or Member State law, the controller or the specific criteria for its nomination may be provided for by EU or Member State law *(Article 4[7] of the GDPR)*.[15]
Data protection by design	The concept of 'Data Protection by design' and 'Data Protection by default' means embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy (*Article 25 of the GDPR*) .[15]
Data Protection Impact Assessment (DPIA)	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. DPIAs are important tools for negating risk, and for demonstrating compliance with the GDPR (*Article 35 of the GDPR*).[17]
Data Protection Officer (DPO)	A Data Protection Officer is a designated person appointed by an organisation to advise on data protection practices. Under the GDPR, a Data Protection Officer is required for public bodies if the organisation performs large-scale processing of sensitive data or performs extensive monitoring of data subjects (*Article 37 – 39 of the GDPR*).[25]

Term	Description of term
Data subject	An individual who is the subject of personal health or social care data, for example, a patient admitted to a hospital or a child receiving the service of a social worker (*Recital 75 of the GDPR*).
Identifier	An identifier is a number assigned by an organisation to an individual to uniquely identify the individual for the purposes of the organisation's operations.
Information Governance	The arrangements that are in place to manage information to support the immediate and future regulatory, legal, risk, environmental and operational requirements of national health and social care data collections.
Personal health information	Personal data related to the physical or mental health of an individual, including the provision or registration of health care services, which reveal information about his or her physical or mental health status (*Recital 35 and Article 4[13] of the GDPR*). The definition of personal health information has been broadened under GDPR to include information on; an individual health identifier, genetic data, biological sample data, in vitro diagnostic test, biometric data such as imaging (*Recital 53 and Article 4[13,14] of the GDPR*). Personal health information relates to an individual who is or can be identified (*Article 4[1] of the GDPR*). Pseudonymised data requires the same privacy provisions as identifiable information if there is a chance that an individual could be identified either from: ▪ the data itself ▪ the data combined with other information freely available to the 'Data Controller' (*Recital 26 and Article 4[5] of the GDPR*).
Privacy	The right of individuals to keep information about themselves from being disclosed; that is, people are in control of others access to themselves or information about themselves. Patients and individuals decide when, where and with whom to share their personal health information.
Privacy Impact Assessment (PIA)	The PIA process is 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. A PIA is best undertaken at the beginning of a project before any significant investment has been made, when the outcome of the PIA can influence the design of the project. A PIA should also be carried out when a change to a project is proposed. Throughout the project, the PIA will need to be

Term	Description of term
	revisited, reviewed and updated when necessary to incorporate changes to the project as it progresses. The term 'Data Protection Impact Assessment (DPIA)' is used in the GDPR and is a mandatory requirement for any high risk processing activity (*Article 35 of the GDPR*).[18]
Processing	The processing of personal health information means performing any operation or set of operations on the information or data, whether or not by automatic means, including: (a) obtaining, recording or keeping the information (b) collecting, organising, storing, altering or adapting the information (c) retrieving, consulting, sharing or using the information (d) disclosing the information or data by transmitting, disseminating or otherwise making it available, or (e) aligning, combining, matching, blocking, erasing or destroying the information (*Article 4[2] of the GDPR*).[18]
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. This definition also includes any proposed amendment(s) to the items listed above that are already in existence. A 'Data Protection Impact Assessment (DPIA)' is a mandatory requirement for each high-risk processing activity (*Article 35 of the GDPR*).[18]
Pseudonymisation	This means the processing of personal data in such a manner that the personal health information cannot be attributed to a service user without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (*Recital 26 and Article 4[5] of the GDPR*).[15]
Risk register	This is a register of risks. It is a tool commonly used to manage the risks throughout a service. It is a means of identifying, assessing, managing and monitoring all significant risks coherently.
Service provider	This term is used in this guidance 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),

Term	Description of term
	private consultant or national data collection. Data protection legislation, including the GDPR, refers to the legal term 'Data Controller' *(Article 4[7] of the GDPR*).
Service user	This term is used in this guidance to describe individuals whose personal health information is potentially being collected, used and disclosed by a service provider. For example: ▪ people who use health and social care services as patients ▪ carers, parents and guardians ▪ organisations and communities of interest that represent the interests of people who use health and social care services ▪ members of the public and communities who are potential users of health services and social care interventions. Data protection legislation, including the GDPR, refers to the legal term 'Data Subject'.[15]
Standard	A standard is a document, established by consensus and approved by a recognised body, which provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

Appendix 2: International evidence

The update of the guidance presented in this document was underpinned by a detailed international review of best practice in this area. This *International Review of Privacy Impact Assessments* is published on the HIQA website. The jurisdictions reviewed in detail were Australia, Canada, New Zealand and the United Kingdom. A high-level review of the European perspective was also undertaken. The focus of the review was to determine the current situation in each country in relation to privacy impact assessments that would provide evidence to inform the update of this guidance. A number of subject areas were examined including an overview of the developments in the jurisdiction, relevant legislation, key organisations, national guidance, the PIA process employed and examples of PIAs conducted in the health and social care setting.

In order to verify the content of the international review, and to gain further insight, key organisations in each jurisdiction were contacted. These include:

- **Australia**
  - Office of the Australian Information Commissioner,
  - The Australian Institute of Health and Welfare.
- **Canada**
  - Office of the Privacy Commissioner of Canada,
  - The Canadian Institute for Health Information.
- **New Zealand**
  - Ministry of Health,
  - The Office of the Privacy Commissioner.
- **United Kingdom**
  - Care Quality Commission,
  - Information Commissioner's Office,
  - NHS Digital,
  - NHS England.

Experts in data protection were contacted in Brussels, Germany and the Netherlands. Some of the key findings in relation to legislation and PIA guidance are highlighted below.

Legislation

Each jurisdiction reviewed has legislation to protect privacy. Australia, Canada and New Zealand have privacy acts, while the UK and the EU have data protection legislation. The European Convention on Human Rights encompasses privacy within the EU, and is legislated for in the UK under the Human Rights Act. Some jurisdictions have further legislation protecting the privacy of health information at a governmental level such as the UK's National Health Service Act and the Health and

Social Care Act; while Australia and Canada legislate for health information privacy at the state, provincial and territorial level. There is currently no legal requirement to undertake Privacy Impact Assessments in Australia, New Zealand, or the UK; however, they are a focus of 'best practice' and are required as part of adherence to certain national standards. PIAs are legally required at a provincial and territorial level in some jurisdictions in Canada.

PIA guidance

In many of the jurisdictions reviewed, such as Australia, New Zealand and the UK, the Information or Privacy Commissioner had responsibility for developing broad guidance on PIAs for all sectors. Sector-specific guidance has been developed for the health sectors in New Zealand(26) and the UK.(27) The development of this PIA guidance has drawn strongly from best practice in other areas (Appendix 3). Some of the PIA guidance documents which were reviewed in greater detail include:

- Australia – *Guide to undertaking privacy impact assessment*. Office of the Australian Information Commissioner(22)
- Canada – *Directive on Privacy Impact Assessment*. Treasury Board Secretariat(28)
- New Zealand – *Privacy Impact Assessment Toolkit*. Office of the Privacy Commissioner(29)
- UK – *Conducting privacy impact assessments code of practice: Data Protection Act.* Information Commissioner's Office.(23)

The requirement for Data Protection Impact Assessment (DPIA) under the new General Data Protection Regulation (GDPR) has resulted in a number of guidance documents being published in Europe. Some of those reviewed include:

- *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. The Article 29 Data Protection Working Party.§(18)
- *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*. The European Data Protection Supervisor (EDPS).(30)
- *A Privacy Impact Assessment Framework (PIAF) for data protection and privacy rights*. The PIAF consortium for the European Commission.(31)
- The Office of the Data Protection Commissioner in Ireland has developed Guidance on Data Protection Impact Assessments (DPIA) in the context of the GDPR.(17)

§Please note these guidelines are being updated and are due to be published in early October 2017.

PIA process

The PIA guidance documents that were identified internationally were reviewed and assessed in order to determine best practice in relation to the PIA process. The number of stages within the PIA process varies in each guidance document, ranging from four steps in the European Data Protection Supervisor toolkit, which focused on privacy as a human right, to 12 steps in the European Privacy Impact Assessment Framework guidance. While the number of steps may vary, the essential components that formed part of each guidance document were included in the five stages outlined in this document. The mapping of the stages used in each of the documents reviewed and how they relate to the stages used in this document can be found in Appendix 3.

Appendix 3: Summary of International evidence (PIA guidance)

Ireland	Australia	Canada	Europe	Europe	Europe	New Zealand	UK
HIQA PIA guidance	**OAIC - PIA Guide[22]**	**TBS - Directive on PIA[28]**	**Article 29 WP - Guidelines on a DPIA [18]**	**EDPS – fundamental right to the protection of personal data toolkit[30]**	**PIAF[31]**	**OPC- PIA Toolkit[29]**	**ICO - Code of practice [23]**
Stage 1 - Threshold assessment	Threshold assessment	Overview and PIA initiation	Assess if processing is 'high-risk' and if a DPIA is mandatory?	Preliminary assessment	Threshold analysis	A brief privacy preliminary analysis	Screening questions- identify the need for a PIA
Stage 2 - Identification of risks: By examining the ▪ privacy management ▪ scope and description ▪ information flows.	▪ Plan the PIA ▪ Describe the project ▪ Identify and consult with stakeholders ▪ Map information flows	▪ Risk area identification and categorisation ▪ Analysis of personal information elements	▪ Systematic description of the envisaged processing ▪ Assessment of the necessity and proportionality of the processing ▪ Views of data subjects or their representatives are sought	▪ Identification of fundamental rights and freedoms limited by the processing of personal data ▪ Define objectives of the measure	▪ Identifying the PIA team and setting terms of reference ▪ Description of the proposed project ▪ Analysis of the information flows and other privacy impacts ▪ Consultation with stakeholders	▪ Gather all the information you need to do the PIA ▪ Sketch out the information flows ▪ Check against the privacy principles ▪ Identify any real privacy risks ▪ Consult with stakeholders	▪ Describe the information flows (how it is obtained, used and retained) ▪ Identify the privacy and related risks against privacy legislation ▪ Consult with internal and external stakeholders

Stage 3 - Analyse and address the risks: ▪ conduct detailed analysis of privacy risks, ▪ develop ways to mitigate them, ▪ Senior management approval.	▪ Privacy impact analysis and compliance check ▪ Privacy management: addressing risks to remove, minimise or mitigate any negative privacy impacts identified ▪ Recommendations	▪ Privacy compliance analysis	▪ Assessment of the risks to the rights and freedoms of data subjects ▪ Measures envisaged to address the risks ▪ Consult supervisory authority when a DPIA reveals high residual risks that cannot be mitigated	▪ Choose option that is effective and least intrusive ▪ Compliance with data protection laws	▪ Risks management ▪ Legal compliance check ▪ Formulation of recommendations	▪ Take action ▪ Manage any risks with using third-party contractors	▪ Identify and evaluate the privacy solutions; reduce or eliminate risk ▪ Cost-benefit analysis of privacy versus project outcomes
Stage 4 - PIA report: ▪ Publish	▪ Report - is an important output of the PIA process.	▪ Summary of analysis and recommendations ▪ Formal approval	▪ Documentation - Provide DPIA report to supervisory authority if required ▪ Publishing is not a legal requirement. Consider publishing report or summary		▪ Preparation and publication of the report	▪ Publish PIA	▪ Sign off and record the PIA outcomes ▪ Approval at right level ▪ Publish report ▪ Circulate to stakeholders

Stage 5 - Incorporating PIA outcomes into the project plan	▪ Respond and review - A PIA should be regarded as an ongoing process		▪ Monitoring and review- periodically or when processing changes		▪ Implementation of recommendations ▪ Revisiting PIA if the project in question changes ▪ External review and or audit	▪ Review and adjust the PIA as necessary as the project develops ▪ Establish better governance structures to manage personal information ▪ Align the PIA with the organisation's existing project-management methodologies ▪ Get an external view of your PIA	▪ Integrate the outcomes into the project plan ▪ Continue to use throughout the project lifecycle

Appendix 4: Privacy Impact Assessment threshold assessment (Stage 1)

Please note this template is available on the HIQA website as an interactive PDF:

1. Contact Details and Overview

Date:

Service provider name:

Project title:

Project lead:

Individual conducting PIA:

Contact details:

Brief overview of the project to include:

- the objective
- whose personal health data will be collected
- who will be collecting, storing and accessing the data
- what operations are envisaged for data collection, storage, access, transfer
- the duration of processing.

2. Checklist - Does the project involve any of the following:

The collection, use or disclosure of personal health information? Regardless of whether the information is identifiable or not.	Yes ☐	No ☐
The collection, use or disclosure of additional personal health information held by an existing system or source of health information?	Yes ☐	No ☐
A new use for personal health information that is already held?	Yes ☐	No ☐
Sharing of personal health information within or between organisations?	Yes ☐	No ☐
The linking, matching or cross-referencing of personal health information that is already held?	Yes ☐	No ☐
The creation of a new, or the adoption of an existing, identifier for service users; for example, using a number or biometric?	Yes ☐	No ☐
Establishing or amending a register or database containing personal health information?	Yes ☐	No ☐
New/innovative use of technology or organisational solutions?	Yes ☐	No ☐
Exchanging or transferring personal health information outside the European Union?	Yes ☐	No ☐
The use of personal health information for research or statistics, whether de-identified or not?	Yes ☐	No ☐
A new or changed system of data handling; for example, policies or practices around access, security, disclosure or retention of personal health information?	Yes ☐	No ☐
Any other measures that may affect privacy or that could raise privacy concerns with the public?	Yes ☐	No ☐

If the answer to one or more of the questions is "yes" then a Privacy Impact Assessment must be undertaken to ensure compliance with privacy legislation. If the answer to all of the questions is "no" it will not be necessary to complete a Privacy Impact Assessment.

3. Recommendations

Individual conducting the threshold assessment:

Is a Privacy Impact Assessment required?	Yes ☐	No ☐

Name:

Signature:

Title:

Date:

Endorsement by Data Protection Officer:

Do you agree with the above Privacy Impact Assessment recommendation:	Yes ☐	No ☐

Name:

Signature:

Title:

Date:

Endorsement by senior management:

Do you agree with the above Privacy Impact Assessment recommendation:	Yes ☐	No ☐

Name:

Signature:

Title:

Date:

Appendix 5: Additional resources relating to Privacy Impact Assessments (PIA)

Key documents identified in the background literature review by jurisdiction:

Australia – *Guide to undertaking privacy impact assessments*. Office of the Australian Information Commissioner.[22] https://www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-undertaking-privacy-impact-assessments.pdf

Canada – *Directive on Privacy Impact Assessment.* Treasury Board Secretariat.[28] http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308

Ireland – *Data Protection Impact Assessment*. Data Protection Commissioner.[17] http://gdprandyou.ie/data-protection-impact-assessments-dpia/

New Zealand – *Privacy Impact Assessment Toolkit* . The Office of the Privacy Commissioner.[29] https://opcwebsite.cwp.govt.nz/news-and-publications/guidance-resources/privacy-impact-assessment/

UK - *Conducting privacy impact assessments code of practice: Data Protection Act*. The Information Commissioner's Office.[23] https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

European Union

- *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*. The Article 29 Data Protection Working Party.[18] http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
- *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*. The European Data Protection Supervisor (EDPS).[30] https://edps.europa.eu/sites/edp/files/publication/17-06-01_necessity_toolkit_final_en_0.pdf
- *A Privacy Impact Assessment Framework (PIAF) for data protection and privacy rights*. The PIAF consortium for the European Commission.[31] http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf

Example reports of PIAs that have been conducted in Ireland:

Privacy Impact Assessment (PIA) for the Individual Health Identifier: Draft for Public Consultation. Health Service Executive.[20]
http://www.ehealthireland.ie/Library/Document-Library/IHI-Documents/PIA-IHI.pdf

Privacy Impact Assessment (PIA) - Summary Report. National Patient Experience Survey Programme.[21]
https://www.patientexperience.ie/app/uploads/2017/07/HIQA-NPESP-PIA-Summary-Final-Report-v1-0-July-2017-2.pdf

Published by the Health Information and Quality Authority.

For further information please contact:

Health Information and Standards Directorate

Health Information and Quality Authority

George's Court,

George's Lane,

Dublin 7,

D07 E98Y

Phone: +353 (0) 1 814 7400

URL: www.hiqa.ie