Health Information and Quality Authority

An tÚdarás Um Fhaisnéis agus Cáilíocht Sláinte

Guidance on Privacy Impact Assessment in Health and Social Care

December 2010

About the Health Information and Quality Authority

The Health Information and Quality Authority is the independent Authority which has been established to drive continuous improvement in Ireland's health and social care services. The Authority was established as part of the Government's overall Health Service Reform Programme.

The Authority's mandate extends across the quality and safety of the public, private (within its social care function) and voluntary sectors. Reporting directly to the Minister for Health and Children, the Health Information and Quality Authority 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 (except mental health services)

Social Services Inspectorate — Registration and inspection of residential homes for children, older people and people with disabilities. Inspecting children detention schools and foster care services. Monitoring day and pre-school facilities[1]

Monitoring Healthcare Quality — Monitoring standards of quality and safety in our health services and investigating as necessary serious concerns about the health and welfare of service users

Health Technology Assessment — Ensuring the best outcome for the service user by evaluating the clinical and economic effectiveness of drugs, equipment, diagnostic techniques and health promotion activities

Health Information — Advising on the collection and sharing of information across the services, evaluating information and publishing information about the delivery and performance of Ireland's health and social care services.

[1] Not all parts of the relevant legislation, the Health Act 2007, have yet been commenced.

Overview of Health Information Function

Health is information-intensive, generating huge volumes of data every day. It is estimated that up to 30% of the total health budget may be spent one way or another on handling information, collecting it, looking for it, storing it. It is therefore imperative 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.

The Health Information and Quality Authority was established under the Health Act, 2007 with the primary objective of promoting safety and quality in the provision of health and personal social services for the benefit of the health and welfare of the public.

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

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. Further to this, it can support a much faster, more reliable and safer referral system between the patient's general practitioner (GP) and hospitals.

Although there are a number of examples of good practice, the current ICT infrastructure in Ireland's health and social care sector, is highly fragmented with major gaps and silos of information which prevents the safe, effective, transfer of information. This results in service users 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 well-being, 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 – the general public, patients and service users, health professionals and policy makers – to make choices or decisions based on the best available information. This is a fundamental requirement for a high reliability healthcare system.

Table of Contents

Executive Summary

The primary mandate of the Health Information and Quality Authority (the Authority) is to drive patient safety in health and social care in Ireland. In respect of health information this also includes ensuring that service users' interests are appropriately protected. This includes the right to privacy, confidentiality and security of their personal health information.

With so much information being collected, used and shared in the provision of health and social care, it is important that steps are taken to protect the privacy of each individual and ensure that sensitive personal health information is handled legally, securely, efficiently and effectively in order to deliver the best possible care.

Privacy Impact Assessments (PIAs) are a common tool used internationally to protect individuals' privacy. PIAs are used across all sectors but are particularly useful for healthcare providers in assisting to identify potential risks around the collection and use of personal health information as this information is categorised as being sensitive. The primary purpose in undertaking a PIA is to protect the rights of service users.

PIA is a process that facilitates the protection and enhancement of the privacy of individuals. Another key benefit of Privacy Impact Assessments is the value and cost savings they can bring to health and social care projects. 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 genuinely influence the development of a project before any significant investment has been made. The cost of risk mitigation at the planning stage of a project is very likely to be considerably less than the possible costs that could be incurred should changes be required to a project following implementation. PIA considers the future privacy consequences of a proposed project that involves the collection and use of personal health information, such as, for example setting up a database for diabetic patients in a hospital. 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 information. The process involves the evaluation of broad privacy implications of projects and relevant legislative compliance. Where potential privacy risks are identified, a search is undertaken, in consultation with stakeholders, for ways to avoid or mitigate these risks.

This document has been developed as a resource to support service providers in protecting the privacy rights of their service users and strengthening governance arrangements around 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.

Part 1 of this document introduces the concept of privacy and the importance of information in providing high quality and safe health and social care services. It provides background information on current legislation and policy in this area and indicates the role of the Authority in this regard. It details the role of 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 around areas to be addressed in identifying real or potential risks to privacy.

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

1. Introduction

1.1. Background

Information is a vital resource in the delivery of high quality and safe health and social care services. The objective of the current Health Service Reform Programme[2] is to deliver better patient care and safety. This means using information – in manual and electronic form - more effectively to improve healthcare outcomes, while ensuring that an individual's control over his or her personal health information is appropriately respected. This requires an examination of how the information is used, the areas where it could be better used and the safeguards needed to ensure appropriate protection(3). However, there is a need to strike an appropriate balance between using personal health information as required to provide appropriate and safe care while continuing to protect the service users' rights to privacy and confidentiality(4).

Under Irish legislation, the right to privacy is protected by, amongst other legislation, the Data Protection Acts 1988 and 2003(1;2). These Acts outline the rights of individuals under eight key principles of data protection and the responsibilities of those who hold and process personal information. The Data Protection Commissioner has a statutory responsibility to implement the terms of the Data Protection Acts and has a wide range of powers which can legally oblige a person holding personal data to comply with the terms of the Acts. The Data Protection Commissioner is responsible for upholding the rights of individuals as set out in the Acts and enforcing the obligations on those holding and processing personal information.

Both the 2001 health strategy, *Quality and Fairness a Health System for You* (4) and the *National Health Information Strategy 2004*(5) (NHIS) highlight the importance of safeguarding the privacy and confidentiality of personal health information by the establishment of a legislative framework - the Health Information Bill. The Health Information Bill, due to be published in 2011, is expected to build on the legislative provisions already in place and seen to be working well – primarily those outlined in the Data Protection and in the Freedom of Information Acts 1997 and 2003. It is anticipated that the Health Information Bill will provide a set of rules to ensure the full and proper use of health information while protecting the privacy of the individual. The right of service users to have their privacy respected is a key underlying principle.

In advance of the publication of the Health Information Bill, it remains essential that individual privacy is safeguarded appropriately. The role of the Authority in this is to develop

[2] The Health Service Reform Programme was announced in 2003 by the Department of Health and Children. It addresses a range of reforms to help modernise the health services to better meet the needs of patients. The reforms are designed to achieve a health service that provides high quality care, better value for money and improves health care management.

an information governance framework for health information to help ensure that the privacy rights of individuals are respected.

The 2001 health strategy proposed the establishment of the Authority and the Authority's areas of responsibility. The strategy states that, among other things, the Authority will promote a common approach to security, privacy and confidentiality[4] of health information. Similar to the 2001 health strategy, the NHIS sets out the role of the Authority in this regard. Part of this role involves ensuring that a national approach is taken to the collection, processing, analysis, availability, use and sharing of health information within a legislative and governance framework that safeguards confidentiality and privacy[5].

The 2008 *Report of the Commission on Patient Safety and Quality Assurance*[6] and the Authority's *Draft National Standards for Safer Better Healthcare*[7] further highlights the need to protect the privacy of service users. The Commission on Patient Safety and Quality Assurance published its report *Building a Culture of Patient Safety*[6] in 2008. This report explains the importance of sharing of data, knowledge and expertise in order to ensure that the health service can operate effectively. However, this should be subject to the appropriate safeguards being in place to protect the privacy of an individual's health information from unauthorised access or disclosure. The Commissions' report details the major contributions that the effective use of health information can make to improving patient safety and quality of care. One of these contributions is the enhancement of privacy, confidentiality, integrity and security of patient information.

In September 2010 the Authority launched a consultation document on *Draft National Standards for Safer Better Healthcare*[7]. Privacy features as a key element of Theme 7 of the Standards, "Use of Information", and requires that service users' dignity, privacy and autonomy are respected and protected. For example, the first criterion under standard 7.1 states that service providers must protect the security, privacy and confidentiality of personal health information and the right of service users to access their own records[7].

1.2. The Role of PIAs

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. The primary purpose in undertaking a PIA relating to health information is to protect the rights of patients and service users. PIAs form a fundamental part of information governance in assuring that patients' rights to privacy and confidentiality are appropriately protected.

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. This increases awareness among professionals and creates a culture where maintaining personal health information privacy is a priority.

2. Privacy

2.1 What is privacy and why is it important?

While it is difficult to define privacy formally, the Data Protection Commissioner in a booklet aimed at the second level education sector has described privacy simply as the right to be left alone[8]. In terms of information about an individual, privacy can be described as the right of individuals to keep information about themselves from being disclosed[9]. However, in order to provide safe and effective health and social care, health information must be collected, used and disclosed even though it is one of the most sensitive forms of personal information. Creating a balance between respecting individual privacy and providing safe and effective care is the difficult but very important task faced by health and social care organisations. Personal health information has become a valuable commodity and it is vital that it is treated as such.

2.2 Service users rights in relation to privacy

Each individual accessing health and social care has specific rights in relation to their privacy. The Data Protection Commissioner highlights the privacy related rights of each individual very clearly in the Data Protection Acts of 1988 and 2003. The Acts state that each individual, whose personal information is collected, used or disclosed by another individual or organisation is entitled to:

- feel sure that their personal information is kept safely and securely
- check that the information held about them is factually correct, complete and up to date
- have their information used only for its original stated purpose(s)
- know who has access to 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.

2.3 Service providers responsibilities in relation to privacy

The Data Protection Commissioner defines a data controller as any individual (e.g. a GP) or organisation/service provider (e.g. a hospital, the HSE etc) that collects, uses or discloses personal information. Under data protection rules, data controllers are obliged by law to protect the privacy of the individuals whose personal health information they collect.

Each data controller must uphold the rights of the individual as above and is responsible for ensuring that they only hold personal information that is actually needed, that they hold it securely and only for as long as it is needed and for the specific purposes for which they obtained it.

3. Privacy Impact Assessments (PIAs)

3.1 What is a PIA?

Privacy can be defined as the right of individuals to keep information about themselves from being disclosed[9]. Service providers, as data controllers, are obliged to uphold this right. The collection, use, storage and disclosure of personal health information is necessary to the provision of effective health and social care. However, this can present significant risks to the privacy of the individual especially as ever-increasing amounts of personal health information are processed. It is vital that service providers assess possible privacy risks in relation to the collection, use, storage and disclosure of personal health information at the planning stage of projects. By identifying any significant risks to privacy posed by a new initiative, it should be possible to mitigate or reduce these risks without necessarily impacting negatively on the success of the initiative. It will also drive an initiative to clearly identify what precise data are required and for what purpose, which will assist in focusing resources.

PIA is a process that facilitates the protection and enhancement of individuals' privacy. It considers the future privacy consequences of a proposed project or initiative. 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 information. The process involves the evaluation of broad privacy implications of projects and relevant legislative compliance. Where potential privacy risks are identified, a search is undertaken, in consultation with stakeholders, for ways to avoid or mitigate these risks. Conducting PIAs should be embedded as part of the project management framework so that the management of privacy risk is an ongoing process. Therefore, the PIA should be reviewed and updated throughout the duration of the project[10].

3.2 International PIA experience

The Authority has published an International Review of PIA practice[10] in other jurisdictions. In each of the countries examined, PIAs are increasingly coming to the fore when undertaking projects that involve the collection, use, disclosure or processing of personal information. Although they are not yet prominent in Europe, PIAs are likely to emerge as a matter of policy and culture in the coming years, as they have in the other jurisdictions. Canada, New Zealand and Australia have called for a review of existing legislation to mandate PIAs for projects or initiatives that collect, use or disclose personal information and which may therefore pose a threat to individuals' privacy. The international review revealed that the countries studied have been heavily influenced by each other and have modelled their processes and guidelines on international practices. There is therefore a growing convergence in respect of what constitutes best practice in relation to PIAs.

3.3 Why are PIAs needed?

The Authority has developed this guidance on how to complete a PIA to aid service providers in identifying and addressing privacy risks. The primary purpose in undertaking a PIA relating to health information is to protect the right to privacy of individuals and service users. PIA forms a fundamental part of information governance in assuring that patients' rights to privacy and confidentiality are appropriately protected(10).

Privacy risks are identified during or as part of the PIA process. Each privacy risk is then assessed and actions are planned to reduce or avoid those risks. These actions are recommended in the PIA report with senior management being accountable and responsible for ensuring their implementation.

The benefits of undertaking PIAs include:

- service providers who undertake PIAs appropriately demonstrate that the privacy of individuals is a priority for their organisation, and show commitment to putting the rights of the service user first and the proper handling of their personal health information. This helps to build the trust of the service user in the provider
- PIAs educate service providers about privacy and the rights of the service users. This learning is essential in promoting a culture of information governance in organisations
- service providers can potentially save money by conducting a PIA in the early stages of planning an initiative. Potential privacy risks or issues are much simpler to resolve prior to any significant investment being made
- a clear focus will emerge as to the precise data required for an initiative
- in the event of an unavoidable privacy risk or breach occurring, the PIA report can provide evidence that the service provider acted appropriately in attempting to prevent the occurrence. This can help to reduce or even eliminate any negative publicity and loss of reputation.

3.4 Considerations

A PIA in its own right may not highlight all privacy risks or issues associated with an initiative. 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 correct stakeholders for the assessment, selection of those with the necessary knowledge and skills to carry out the PIA and should involve senior managers in order to implement the recommendations made as a result of the PIA.

It is essential that the PIA is regularly updated to reflect any changes to the direction of the initiative to ensure that all discoverable privacy issues are addressed. A PIA is not intended to manage privacy risks and breaches for established health information systems or initiatives. It is intended to be used as an integral part of the project management process for new initiatives.

4. What this guidance hopes to achieve

The purpose of this guidance document is to assist service providers and individuals undertaking PIAs and in doing so assist them in realising the benefits associated with conducting a PIA. 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.

As the concept of conducting PIAs is new to the Irish health and social care sector, a Sample PIA Report based on this guidance has been developed and is available on the Authority's website for illustrative purposes (www.hiqa.ie).

Part 2: The Privacy Impact Assessment Process

5. Introduction to the PIA Process

5.1. How to use this guide

The purpose of this document is to provide guidance around the process of completing a PIA, from the early stages of determining if it is necessary to undertake a PIA to the final stages of completing and publishing the PIA report.

This guidance document provides step by step assistance through each of the stages in the PIA process and identifies the key areas for consideration. Section 6 outlines the initial step in the PIA process – that is the PIA threshold assessment. Section 7 documents the process for identifying risks and section 8 explores how to approach mitigating or avoiding the risks identified. The final stage in the PIA process, the PIA report, is documented in section 9.

The sections that follow offer practical advice on how to undertake a PIA including template documents and examples of issues that may arise in the process. The tools that are included can be modified to suit particular projects as each will vary in their requirements, extent of privacy risks and depth of PIA necessary.

This guidance does not guarantee compliance with the provisions in the Data Protection Acts 1988 and 2003 or any other legislation governing the collection, use or disclosure of personal information. Advice on compliance with those Acts should be sought from the Office of the Data Protection Commissioner.

This guide is not exhaustive as it would be impossible to write a "one size fits all" guide. Issues may arise in projects that are beyond the scope of this guide or that require even more detailed consideration and analysis. Therefore, service providers must continue to use their good judgement, in parallel with this guide, for each project undertaken involving personal health information. Service providers are encouraged to use this guidance document to implement a PIA process that is appropriate to their particular circumstances.

5.2. The PIA Process

The PIA process involves the evaluation of broad privacy implications of projects and relevant legislative compliance. Where potential privacy risks are identified, a search is undertaken, in consultation with stakeholders, for ways to avoid or mitigate these risks. There are four stages in the PIA process as follows:

- Stage 1 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. This is called a Threshold Assessment

- Stage 2 involves identifying the privacy risks through exploring the scope, information flows and security arrangements of the project

- Stage 3 deals with addressing the risks identified in Stage 2. This is achieved firstly through analysing and assessing them and then looking at ways to avoid them or mitigate them through privacy enhancements

- Stage 4 - the output of the PIA process is a PIA report containing the details of each of the three above elements, where appropriate. The PIA report should be publicly available.

The four stages are outlined in Figure 1 which follows.

5.3. Who should conduct a PIA?

The PIA process should be undertaken by people with the appropriate expertise and knowledge of the project in question. As such, it should generally be undertaken by the project team. It may, however, be appropriate to consult service users as part of the PIA process. The service provider is ultimately responsible for the completion of the PIA and for implementing any changes to the project plan following recommendations for privacy enhancement or mitigation of risks arising from the PIA.

PIAs should be reviewed and approved at a senior level with each PIA report being quality assured by senior management. For example, a PIA for a major national project should be approved by the chief executive officer (CEO) of the Health Service Executive (HSE), a PIA for a new hospital patient administration system (PAS) should be approved by the CEO of the hospital and a PIA for a new general practice management system should be approved by the general Practitioner (GP) or the practice manager.

5.4. When should a PIA be completed?

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 genuinely influence the development of a project before any significant 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 and as such the PIA may need to be revisited. 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.

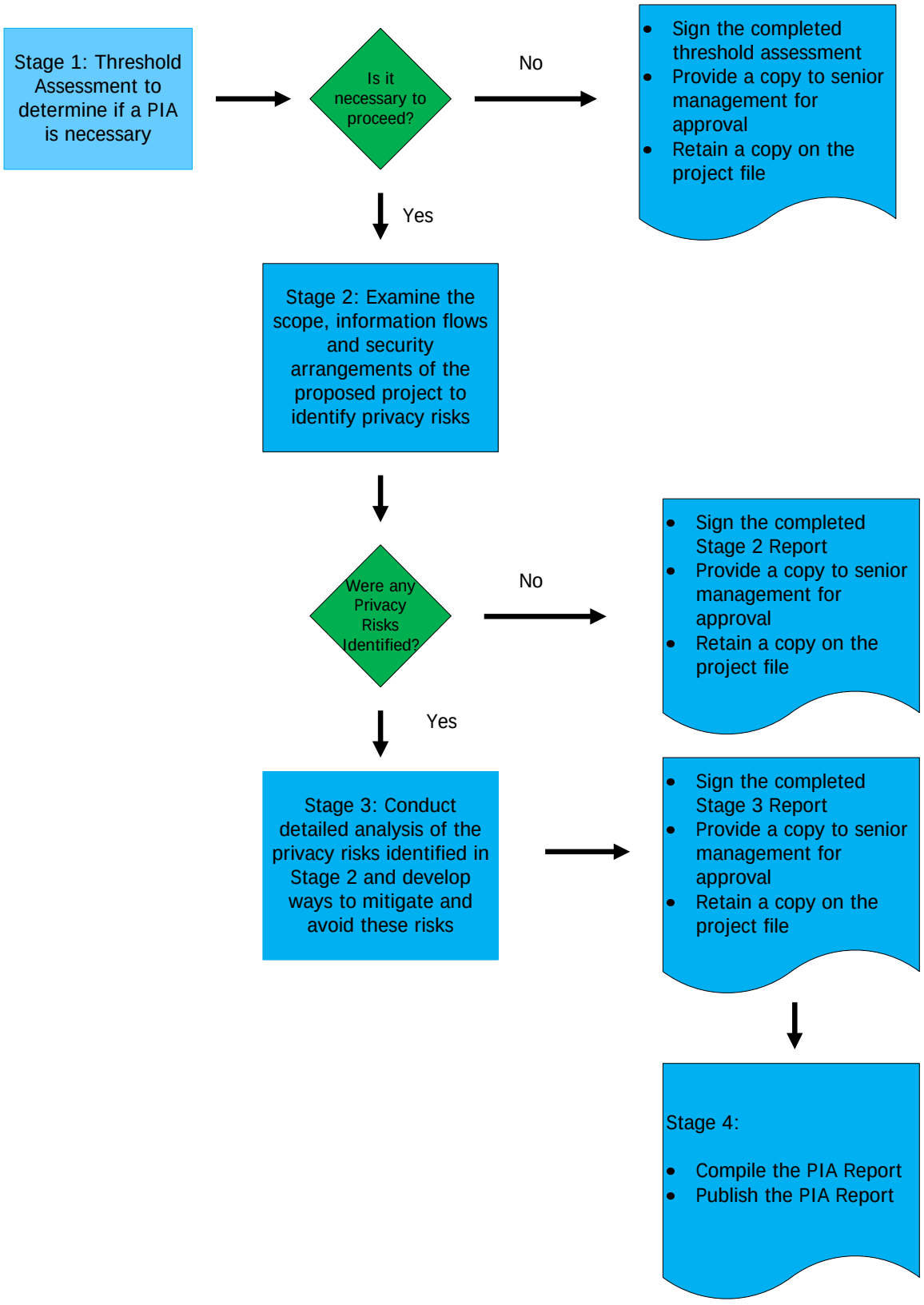


Figure 1 – The PIA Process

6. Stage 1 – PIA threshold assessment

A threshold assessment is a brief, initial assessment of a project, to determine whether its potential privacy impact necessitates a PIA. A threshold assessment should be routinely undertaken for every health information project initiated by a service provider. This applies not only to new projects but also to proposals to amend existing information systems, sources or processes.

The threshold assessment consists of a checklist of eleven questions. The questions focus on the scope of the project and the manner in which personal health information will be used. The questions seek to ascertain, for example, whether the information will be shared or whether the project involves linking or matching of information.

Having completed the threshold assessment there are two possible outcomes for the project team. If the answer to one or more of the questions is "yes" then it is necessary to proceed with the PIA. If the answer to all of the questions is "no" it will not be necessary to complete the PIA process. In either case the completed threshold assessment should be signed and approved by the project lead and senior management and kept on the project file. For example, a threshold assessment for a major national project should be approved by the chief executive officer (CEO) of the Health Service Executive (HSE), an assessment for a new hospital patient administration system (PAS) should be approved by the CEO of the hospital and an assessment for a new general practice management system should be approved by the general Practitioner (GP) or the practice manager.

A template for a PIA threshold assessment is detailed in Appendix 1.

7. Stage 2 – Identification of risks

7.1. Stage 2 overview

If it is deemed necessary to continue with the PIA following the threshold assessment, the process proceeds to Stage 2. Stage 2 involves identifying potential privacy risks through defining how the organisation manages privacy and exploring the project's scope, information flows and security arrangements. If risks are identified at this stage it will be necessary to proceed to Stage 3 – addressing the risks.

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

- privacy management
- a description of the project
- the project type and stage of development
- the scope of the project
- the information flows

Each of these issues is discussed in turn below.

7.2. Privacy management

This section relates to how the service provider manages the privacy of personal health within the organisation. It is not specific to the project undergoing the PIA process but raises issues that must be addressed by any service provider processing personal health information. It explores information governance issues such as data protection and confidentiality, and staff awareness of the policies that are in place. It also examines issues around education and training of staff, and accountability for the handling of personal information, which are key information governance management issues. As this section relates to the service provider generally, and not to any specific project, it is likely that it will only need to be completed for the service provider's first PIA, although it will need to be reviewed and updated regularly. This can significantly reduce the time input required to complete subsequent PIAs providing that the privacy management documentation is kept up-to-date.

Suggested questions that relate to the service provider's privacy management are outlined below. When answering the questions, service providers should indicate whether a particular policy is in place and, if not, the current stage of development for that policy.

- Is there a privacy policy in place that outlines the safeguards employed to protect service users' privacy and confidentiality?
- Is there a statement of information practices setting out the types of information collected, how it is used, if it is shared and how service users can access information held about them?
- Is the service provider compliant with the principles of data protection as outlined in the Data Protection Acts 1988 and 2003[1;2]? Is the service provider the legal data controller for all personal data within the scope of the initiative?
- Is there a records management policy in place that includes a retention and destruction schedule? This should outline how long particular types of information are held for and the process around the secure disposal of both paper and electronic records
- 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 there an appointed privacy or information governance contact person?
- Is there a privacy breach management action plan in place?
- Are employees or agents with access to personal health information provided with training related to privacy protection and confidentiality requirements?

7.3. A 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.

The project description should address the following:

- details of the service provider or individual proposing the project
- the overall aims of the project (including how it ties in with the service provider's functions or activities)
- the drivers for or reasons behind the project
- the scope or extent of the project (whether it is national, regional or local)
- any links with existing projects or programmes.

7.4. The project type and the stage of development

The project type and the stage of development should be documented. Documenting the type of project may lead a service user to the conclusion that a PIA is only necessary on one particular aspect of the project. Further, if the project is incremental it may raise issues around the existing system that need to be addressed.

It is important also to consider and document the current stage of the project. For example, if a project is at a conceptual stage all of the information that is necessary to complete the PIA may not yet be available. This may mean that the PIA may need to be revisited as the project develops and decisions are made. If completing a PIA at the conceptual stage, the team may not yet precisely know what the information flows will be or to whom it will be necessary to disclose the information. Any questions that cannot be answered will need to be revisited as the project develops in order to ensure that all potential privacy risks that may arise are fully addressed.

If the proposed project involves modifications to an existing system, the project team should first describe the existing system and then the proposed changes. Any detail of prior PIAs undertaken in relation to the existing system should also be included. If a PIA was not undertaken, it may be appropriate to consider whether one should be undertaken now.

This section should address such questions as:

- Is this a new project?
- Is this an alteration or an addition to an existing project?
- What is the stage of development of the project?

7.5. The scope of the project

It is important to explore the scope of the project to determine how far-reaching its impact is likely to be. Exploring the scope of the project examines the extent to which a project involves the collection, use or disclosure of personal information. 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. This can be the general population in respect of a national project or the population of service users 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.

This section should address such questions as:

- What information is to be collected?
- Outline why each element of the data set is necessary
- Are the service users aware of the proposed collection, use and disclosure of their personal information? Identify and describe what information is given and how it is given
- Have the service users consented to their personal information being used in this manner? Does the project comply with the consent requirements of the Data Protection Acts? Describe the consent process
- Identify and describe:
  - All the uses of the personal information
  - How these uses relate to the purpose for which the information was collected
  - Any changes to the purpose for using the information after it is collected
  - Measures in place to prevent use for other purposes
- Identify and describe any potential sharing of the information and how the service user has been informed of this
- Is it a possibility that the information will be linked or matched with an existing or proposed system? If yes please provide details
- Does the project, system or initiative involve assigning or using an identifier or using an existing identifier for a new purpose? If yes please provide details.

These questions relating to the scope of the project serve to focus the areas for consideration, but 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.

In some situations defining the scope of information to be collected may result in the project team making changes to the scope or certain other aspects of the project that may raise a risk but are unnecessary to the success or completion of the project. For example, when documenting what information is required as part of the project and identify the rationale for this information, the project team may realise that certain data elements are not necessary for the project to be a success. Therefore, the risk associated with collecting unnecessary information and its subsequent disclosure can be eliminated at this stage of the PIA.

7.6. Information flows

This section is designed to assist in producing a clear picture of the project's information flows and in doing so draw out some possible areas where privacy risks may arise. This section essentially maps the flow of information from the time it is collected, through its use and disclosure if appropriate. It raises questions around how the personal health information will be handled and used, the purpose for its collection, methods of disclosure and safeguards in place to protect privacy. Sample questions to identify potential risk for the information flows are:

- How is the information to be collected?
- What are the proposed uses of the information?
- Will the information be disclosed? To whom? What precautions are in place to prevent inappropriate disclosure?
- Will the data subjects have access to the information and have the opportunity to have any erroneous information about them corrected?
- What security measures will be taken to protect the information from loss, unauthorised access, use, modification, disclosure or other misuse, including how data is transferred from sites or systems?
- Identify and describe the retention and destruction practices to be employed in the project.

As is the case for the sample questions around scope, 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.

7.7. 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 actual or potential privacy risks.

If no privacy risks have been identified, a copy of the Stage 2 assessment should be signed by the project team and approved by senior management as appropriate. For example, for a major national project, approval of the chief executive officer (CEO) of the Health Service Executive (HSE) is required, for a new hospital patient administration system (PAS), approval of the CEO of the hospital is required and for a new general practice management system,

approval of the general Practitioner (GP) or the practice manager is required. A copy should be kept on the project file and made available upon request.

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. In some cases it may be necessary to balance the risks to privacy of personal information against the public good while having regard to legal requirements in this area. This will require an in-depth analysis of certain aspects of the project and consultation with stakeholders who will be affected, which may include service users the general public.

8. Stage 3 – Addressing the risks

Risks to privacy can arise in many circumstances and in relation to many different types of health information projects involving the collection, use or disclosure of personal health information. The purpose of this stage of the PIA process is to 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 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. Stage 3 of the PIA process should be reviewed and approved by a member of senior management.

8.1. Analyse the risks

Risk analysis is about developing an understanding of the risk. It has been defined as a systematic process to understand the nature of and to deduce the level of risk[(11)]. In analysing the risks it is necessary to determine the consequences and the likelihood of a particular event occurring, thereby determining the level of risk. Analysing risks is not a once off exercise - it is part of a process that should be repeated whenever there is a change in the circumstances that affect a risk[(12)]. In the case of health information projects service providers must consider the consequences of the event occurring, both to service users and to the service and also the probability of it occurring. This will enable service providers to rate the risk accordingly.

Sample questions for consideration as part of this stage include:

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

Service providers should follow the processes outlined in their risk management policies for this section of the PIA. 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 consequences and likelihood[(12)]. A sample risk matrix is presented in Figure 2.

A risk matrix can be used to capture the probability of the event occurring and the likely 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 service users involved this would be recorded as a high risk which would impact the progress of the project.

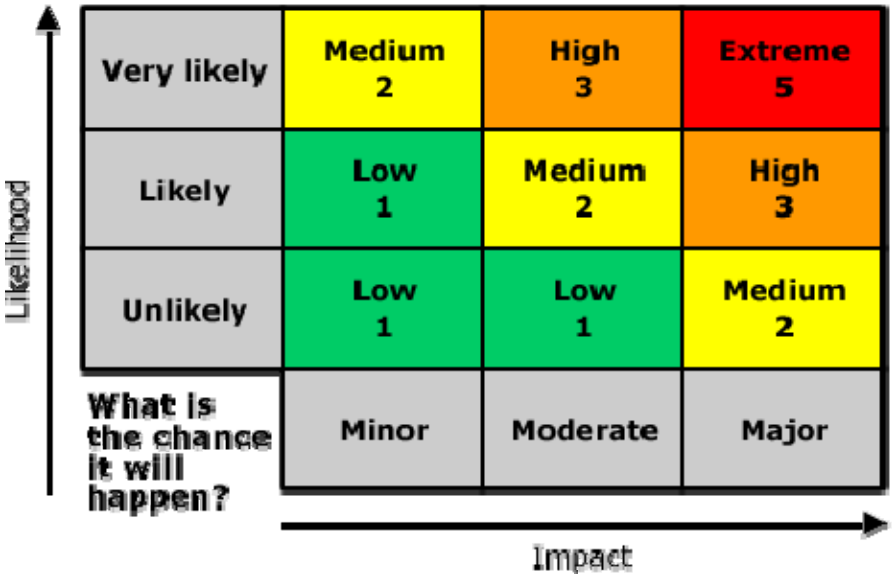


Figure 2 – Sample risk matrix structure [taken from the Australian Transaction Reports and Analysis Centre (AUSTRAC)][13]

The use of a risk matrix enables risks to rated based on the likelihood that they will occur (the vertical line) and the likely impact they would have if they were to occur (the horizontal. The risk matrix can therefore be used to aid decision making in view of the overall level of risk.

If it is very likely that an event will occur and this would have a moderate impact, the risk would be rated as high (represented in the orange box above as “High 3”). The risk of any project staff turnover during the lifetime of the project can be considered within a risk matrix. If the duration of the project is long, then it is very likely that one or more of the people involved in the project may leave the organisation. The impact of this would be moderate, assuming that a replacement can be found in a reasonable timeframe. When this risk is applied to the matrix above, the result of “High 3” is returned.

8.2. Addressing the risks

Following the analysis of each risk (highlighted in Stage 2 of the PIA process) the next step is to identify ways to reduce or eliminate the possibility of each risk occurring.

The positive impacts of risk elimination should always be balanced against how the goals of the project will be affected. Selecting the most appropriate option involves balancing the costs of implementing this option against the benefits derived from it[11]. 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 cost of risk mitigation at the planning stage of a project is very likely to be considerably less than the possible costs that could be incurred should changes be required to a project following implementation.

Examples of proposed actions include:

- do nothing about the risk
- abandon the project completely
- amend the proposed project such that the risk is entirely removed
- remove an aspect of the risk, thereby reducing its possible impact
- employ security measures such as encryption or role based access controls to address security concerns
- introduce an opt out mechanism to allow individuals not to have their personal health information processed or included in the system, thereby eliminating the risk to their data
- a combination of the above.

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 reasoning behind the choices made should be clearly explained in supporting documentation. The actions proposed and approved by senior management should contribute to the risk management aspect of the project so that they are continually monitored as the project evolves.

If, having gone through this process, there is a residual or remaining risk, which cannot be mitigated, the project team must decide whether or not it is acceptable to continue with the project. If a decision is made to continue with the project it must be possible to manage the risk to an acceptable level. Any residual risks should be documented in the service provider's risk register[3], which should be reviewed, updated and managed on a regular basis by the project team and the senior management.

Consultation with stakeholders and members of the public about the privacy risks associated with the project can prove valuable. Through consultation, the level of impact some privacy risks could have can be discovered, which can lead to simpler ways to mitigate risks. The consultation can also be of benefit by enabling stakeholders to suggest ways to reduce privacy risks.

Fresh input on the perceptions of the severity of each risk can be gathered together with the possible steps that could be taken to mitigate these risks. It is more likely that consultation

[3] A risk register is a tool for creating and maintaining a repository of risk information in an organisation[(11)]

with stakeholders will be necessary for large scale health information projects with high risks to the privacy of personal health information.

Feedback gained and any changes made to a project as a result of stakeholder engagement should be included in the PIA report. Stage 3 of the PIA process should be reviewed and approved by a member of senior management from within the organisation. For example, a PIA for a major national project should be approved by the chief executive officer (CEO) of the Health Service Executive (HSE), a PIA for a new hospital patient administration system (PAS) should be approved by the CEO of the hospital and a PIA for a new general practice management system should be approved by the general Practitioner (GP) or the practice manager.

9. Stage 4 - the PIA report

The final output of a PIA is a report which details the proposed project, the steps that were undertaken as part of the PIA process and any subsequent recommendations. It should therefore contain the outputs of stages 1, 2 and 3 of the PIA process. 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. The publication of PIA reports builds a culture of accountability and transparency and inspires public confidence in the service provider's handling of personal health information.

There are a number of benefits to preparing and publishing a PIA report, primarily to the service provider compiling it but which also extend further. These 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 service users to inform themselves of the way their 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.

The structure and format of the report will vary depending on the project and its particular specifications. However, the report must at a minimum convey the following:

- a detailed description of the project including the objectives and justification for the project
- an overview of the PIA process undertaken explaining the outcome at each of the stages
- a copy of the threshold assessment form
- an overview of Stage 2 of the PIA process, with an emphasis on the scope and information flows of the project
- a description of the specific risks that have been identified
- a discussion of alternatives considered to mitigate or avoid these risks and a rationale for the decisions made
- a description of the privacy design features adopted to safeguard privacy
- details of any consultation that took place with stakeholders, service users or the general public
- an outline of any remaining risks that could not be resolved and a business case justifying why it has been decided to accept these risks and proceed with the project and the likely implications for the public or service users involved.

The focus of a PIA report should be on the needs and rights of individuals whose personal health information is collected, used or disclosed. As such, completed PIA reports should be published in an accessible manner and location and be presented in a non-technical and reader-friendly format. The report should be understandable to the general public as a stand-alone document.

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 process, the privacy risks of the project and the steps taken to mitigate those risks. This is an important step in increasing accountability for the handling of personal health information and its protection. For example, a PIA for a major national project should be approved by the chief executive officer (CEO) of the Health Service Executive (HSE), a PIA for a new hospital patient administration system (PAS) should be approved by the CEO of the hospital and a PIA for a new general practice management system should be approved by the general Practitioner (GP) or the practice manager.

10. Conclusion

PIAs are used across all sectors but are particularly important in protecting personal health information as this is highly sensitive information. The primary purpose of undertaking a PIA relating to health information is to protect the rights of service users.

This document has been developed as a resource to support service providers in protecting the privacy rights of their service users 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 completed this guidance, the Authority will continue to develop and publish additional documents to support improvements in information governance and protecting the rights and interests of health and social care service users.

11. Glossary

In the context of this guidance document the following definitions apply:

COLLECT
in the context of *processing*, means to gather, acquire, receive or otherwise obtain information[14]

CONSENT
freely given, specific and informed indication of the data subject's wishes to use their personal health information[15]

DATABASE
refers to an application that manages data and allows fast storage and retrieval of that data

DATA MATCHING
relating or combining personal health information with other information from two or more sources (whether in electronic databases or otherwise) for a purpose for which the personal health information was not originally collected[14]

DE-IDENTIFIED INFORMATION
refers to data or information that cannot be linked to any particular individual, i.e. the data subject cannot be identified from the information either on its own or in conjunction with additional information

IDENTIFIER
a number assigned by an organisation to an individual to identify uniquely the individual for the purposes of the organisation's operations[16]

INFORMATION GOVERNANCE
a strategic framework that brings coherence and transparency to information initiatives and which is responsive to the spectrum of issues and concerns of those involved. Issues such as information sharing, health surveillance, quality assurance, confidentiality, privacy, records management, freedom of information and data protection are all included

PERSONAL INFORMATION[1]
data relating to an individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller

The term **personal health information** is broad and includes such matters as personal information relating to the physical or mental health of the individual, as well as any genetic data or human tissue data that could be predictive of the health of the individual or his or her relatives or descendants. In essence it covers any information relating to an individual that is collected for or in connection with the provision of a health service

POPULATION HEALTH REGISTRY
means a scheme for the processing of personal health information relating to individual cases of a particular disease, illness, disability or other health condition and of a defined population[17]

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/individuals decide when, where and with whom to share their personal health information[9]

PRIVACY IMPACT ASSESSMENT (PIA)
a process designed to identify and address the privacy issues of a particular initiative. 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 that have been identified. A PIA is best undertaken at the outset of a project before any significant investment has been made and the outcome of the PIA can influence the progress of the project

PROCESSING
of or in relation to personal health information means performing any operation or set of operations on the information or data, whether or not by automatic means, including:[14]

(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

but does not include any operation or set of operations anonymising such information

PROJECT
may mean any proposal, review, system, programme, process, application, service or initiative that includes the processing of personal information. For the purpose of this guidance document it is also taken to mean a proposed amendment to any of the items listed above that are already in existence

SERVICE PROVIDER
any agency, practice, hospital, organisation or individual (where that individual is acting as a legal entity e.g. GP, private consultant) proposing to undertake a project involving the collection or processing of personal health information

SERVICE USER
this term is used to describe[18]:

- 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

STANDARD
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[19].

References

(1) The Data Protection Act. 1988. Available online from: http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html.

(2) The Data Protection (Amendment) Act. 2003. Available online from: http://www.dataprotection.ie/documents/legal/act2003.pdf.

(3) The Department of Health and Children. *Discussion Document on Proposed Health Information Bill* [Online]. Available from: http://www.dohc.ie/consultations/closed/hib/discussion_paper.pdf. Accessed on: 28 September 2009.

(4) The Department of Health and Children. *Quality and Fairness: A Health System for You*. 2001. Available online from: http://www.dohc.ie/publications/quality_and_fairness.html.

(5) The Department of Health and Children. *Health Information - A National Strategy*. http://www.dohc.ie/publications/pdf/nhis.pdf?direct=1: 2004. Available online from: http://www.dohc.ie/publications/nhis.html. Accessed on: 29 July 2009.

(6) The Commission on Patient Safety and Quality Assurance. *Building a Culture of Patient Safety*. 2008. Available online from: http://www.dohc.ie/publications/pdf/en_patientsafety.pdf?direct=1. Accessed on: 30 September 2009.

(7) The Health Information and Quality Authority. *Draft National Standards for Safer Better Healthcare*. 2010. Available online from: http://www.hiqa.ie/media/pdfs/Safer_better_care_draft_standards_A4.pdf.

(8) Office of the Data Protection Commissioner. *Sign Up, Log In Opt Out: Protecting your privacy and controlling your data*. 2007. Accessed on: 30 September 2010.

(9) Erickson, J. and Millar, S. Caring for Patients while Respecting their Privacy: Challenges of Maintaining Privacy and Confidentiality. *The Online Journal of Issues in Nursing.* 2005; 10(2): Available online from: http://www.medscape.com/viewarticle/506840_4. Accessed on: 21 June 2010.

(10) The Health Information and Quality Authority. *International Review of Privacy Impact Assessments*. 2010. Available online from: www.hiqa.ie.

(11) Standards Australia and Standards New Zealand. *Australian/New Zealand Risk Management Standard AS/NZS 4360:2004*. 2004. Available online from: http://www.ucop.edu/riskmgt/erm/documents/as_stdrds4360_2004.pdf.

(12) The National Standards Authority of Ireland. *National guidance on implementing I.S. ISO 31000:2009 Risk Management - Principles and guidelines*. 2010.

(13) The Australian Transaction Reports and Analysis Centre (AUSTRAC). *Risk management - A tool for small-to-medium sized businesses*. 2010. Available online from: http://www.austrac.gov.au/files/risk_management_tool.pdf. Accessed on: 30 June 2010.

(14) The Department of Health and Children. *Draft Heads of Health Information Bill*. 2009.

(15) The Office of the Data Protection Commissioner. *Data Protection Guidelines on Research in the Health Sector*. 2007. Available online from: http://www.dataprotection.ie/documents/guidance/Health_research.pdf. Accessed on: 31 August 2009.

(16) Privacy Act (Australia). 1988.

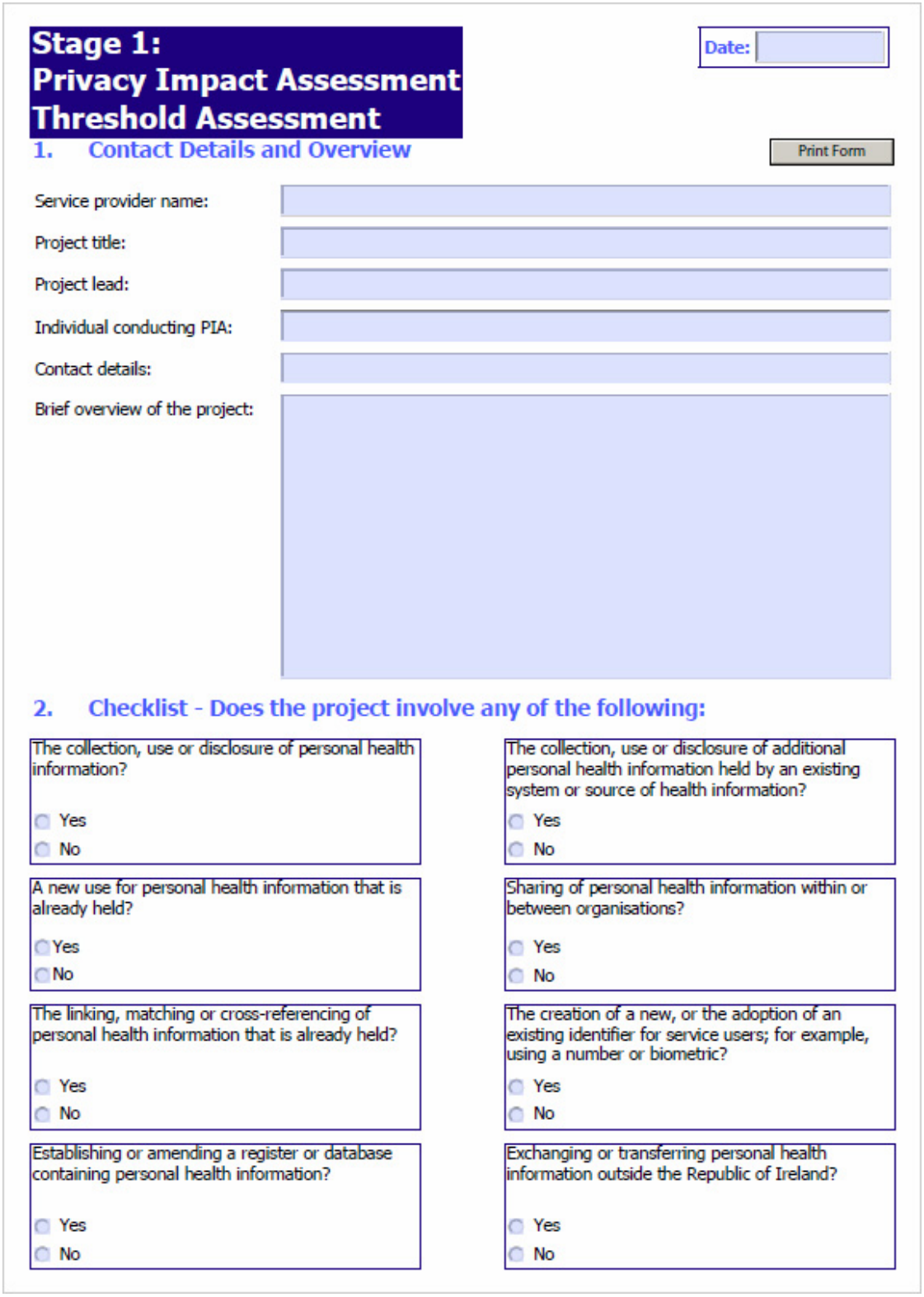
(17) Health (Provision of Information) Act. 1997.

(18) The HSE and the Department of Health and Children. *National Strategy for Service User Involvement in the Irish Health Service*. 2008. Available online from: http://www.hse.ie/eng/services/Publications/Your_Service,_Your_Say_Consumer_Affairs/Strategy/Service_User_Involvement.pdf. Accessed on: 27 September 2010.

(19) International Organisation for Standardisation. *ISO/IEC Guide 2:2004*. 2004. Available online from: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39976.

Appendix 1 – Stage 1: PIA threshold assessment

This form is also available as an interactive resource from www.hiqa.ie



Stage 1:
Privacy Impact Assessment
Threshold Assessment

Date:

1. Contact Details and Overview

Print Form

Service provider name:

Project title:

Project lead:

Individual conducting PIA:

Contact details:

Brief overview of the project:

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

The collection, use or disclosure of personal health information?
- 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

Exchanging or transferring personal health information outside the Republic of Ireland?
- Yes
- No

The use of personal data 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.
If the answer to all of the questions is "no" it will not be necessary to complete a Privacy Impact Assessment.

3. Recommendation

Individual conducting the threshold assessment:

A Privacy Impact Assessment:

- is required
- is not required

Name:
Signature:
Title:
Date:

Endorsement by senior management:

Privacy Impact Assessment recommendation:

- Agree
- Disagree

Name:
Signature:
Title:
Date:

Published by the Health Information and Quality Authority.

For further information please contact:

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

Phone: +353 (0) 1 814 7400
URL: www.hiqa.ie